DEVOPS CONFIGURATION MANUAL

Basic Calculator Webapp

Table of contents :

Tools Used:

1. Maven
2. JUnit
3. Git
4. Jenkins
5. Docker
6. Rundeck
7. ELK

Github Repository :

https://github.com/utsavcoding/Calculator-Devops

Docker Hub Repository :

https://hub.docker.com/repository/docker/utsavcoding/calculator-docker

WorkFlow For Entire Configuration:

1. Jenkins will pull the code from github account.
2. Jenkins will build the pulled code from github and execute all the test cases.
3. A docker Image will be created and pushed to docker hub.
4. It will trigger a rundeck job which will fetch the image from docker hub and run it as a docker container on the server node or host.
5. For continuous monitoring elasticsearch, filebeat and kibana is installed in the host system.

Configuration :

1. **Github:**
   Install maven and git. Create a maven web project and write the calculator program.
   To make a package of the code run the following commands:

   mvn clean install

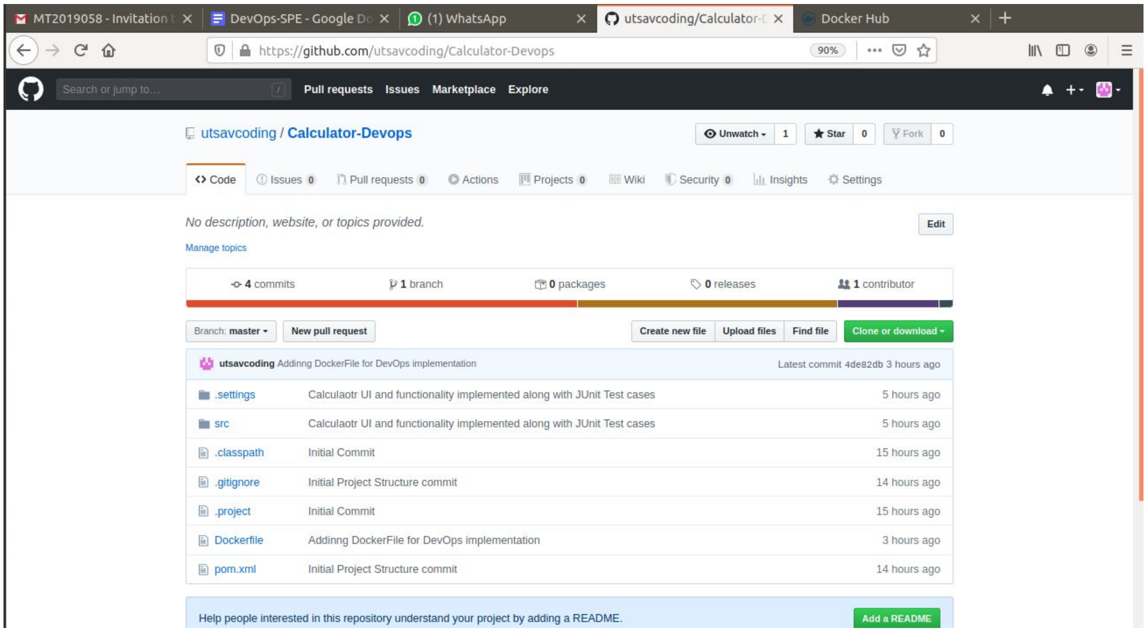
   After executing the above commands automatically a target folder is created which contains our artifact which is a war file. Create a public repository in GitHub and push code to repository using the following commands:

   git add .

   git commit -m “commit message”

   git push

   The image below shows the GitHub repository after the code is pushed to the repository.



No description, website, or topics provided.

4 commits | 1 branch | 0 packages | 0 releases | 1 contributor

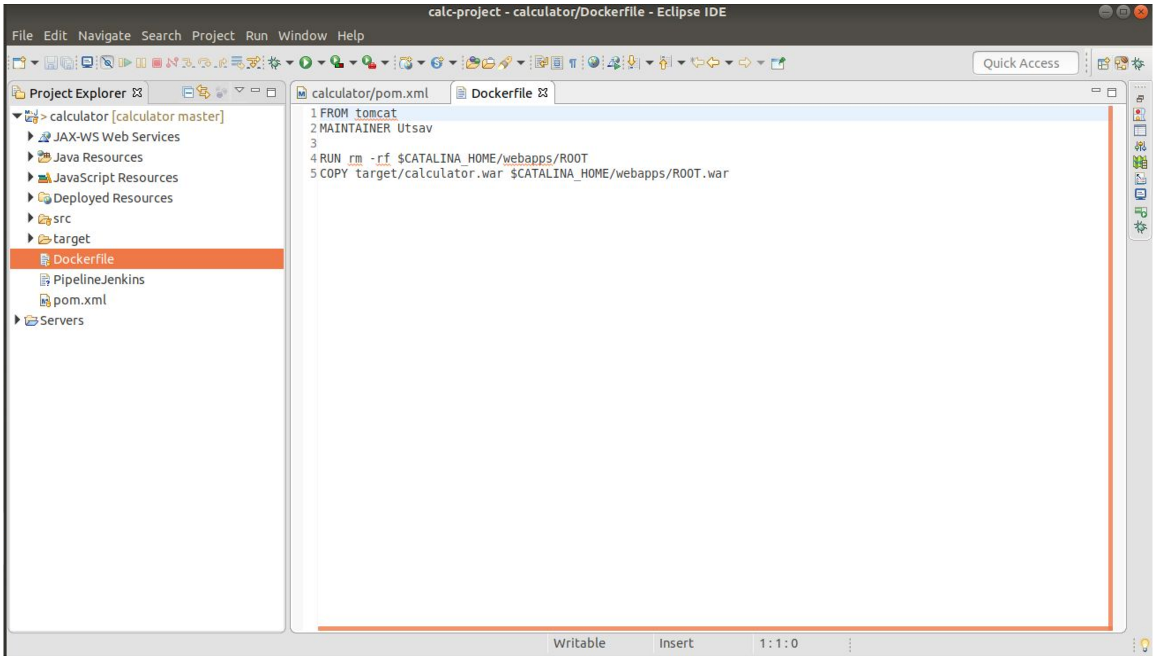
utsavcoding Addinng DockerFile for DevOps implementation — Latest commit 4de82db 3 hours ago

.settings	Calculaotr UI and functionality implemented along with JUnit Test cases	5 hours ago
src	Calculaotr UI and functionality implemented along with JUnit Test cases	5 hours ago
.classpath	Initial Commit	15 hours ago
.gitignore	Initial Project Structure commit	14 hours ago
.project	Initial Commit	15 hours ago
Dockerfile	Addinng DockerFile for DevOps implementation	3 hours ago
pom.xml	Initial Project Structure commit	14 hours ago

Help people interested in this repository understand your project by adding a README.

2. Docker Hub:

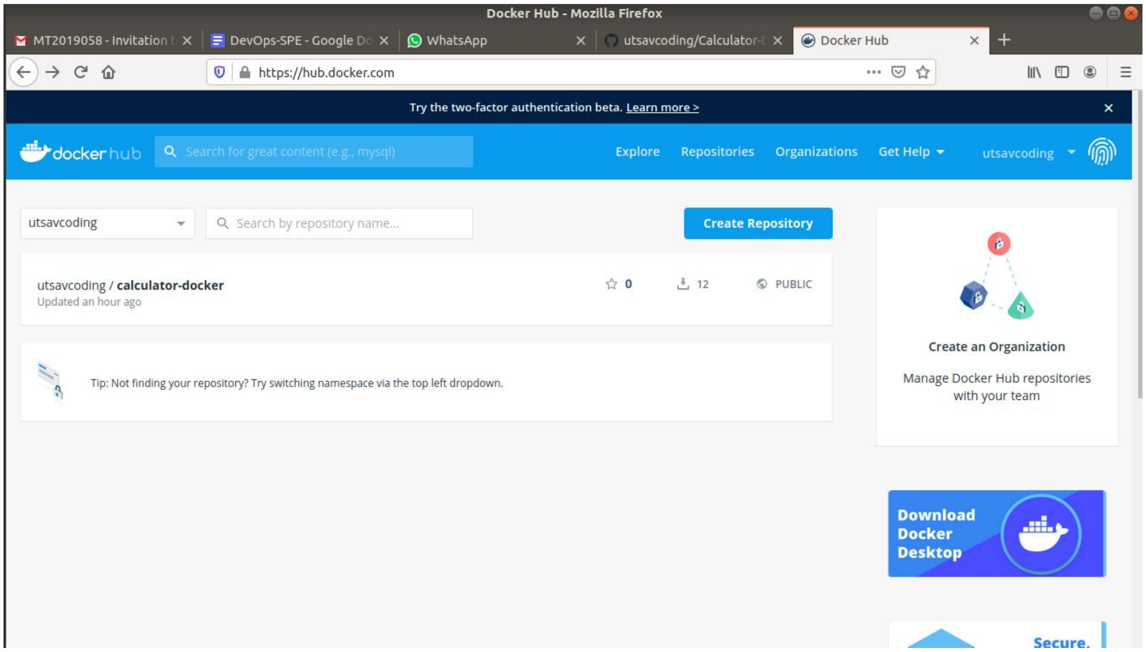
To create a docker image create a docker file inside the project.



```
FROM tomcat
MAINTAINER Utsav

RUN rm -rf $CATALINA_HOME/webapps/ROOT
COPY target/calculator.war $CATALINA_HOME/webapps/ROOT.war
```

.

Docker hub is a repository for all docker images. Create a docker hub account and a repository where docker image will be pushed for the calculator program. Below is the screenshot of docker hub repository used for this project.



utsavcoding

utsavcoding / **calculator-docker**
Updated an hour ago

☆ 0 | 12 | PUBLIC

Tip: Not finding your repository? Try switching namespace via the top left dropdown.

3. **Rundeck:**

Download rundeck_3.2.4.20200318-1_all.deb and run below commands -

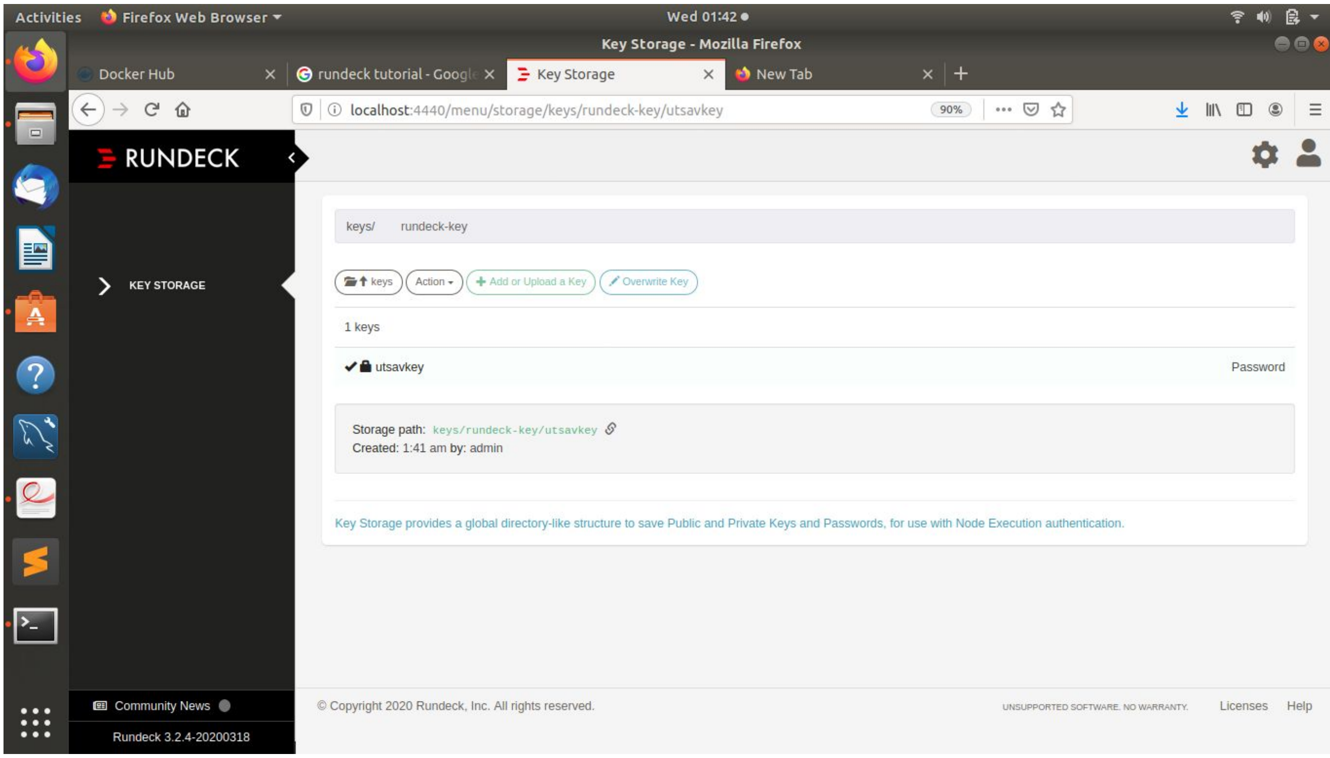
- Install rundeck -

  sudo dpkg -i rundeck_3.2.4.20200318-1_all.deb
- Start rundeck-

  sudo service rundeckd start
- Check http://localhost:4440/
- Create key storages for all the nodes where the project will be deployed.

  Goto Rundeck Setting→Key Storage→Add Or Upload a key. Select the key type as Password.Type a key name(any name) and key password(this will be the node password,i.e our machine password).

  Below is a screenshot of key after creation.



Storage path: keys/rundeck-key/utsavkey

Created: 1:41 am by: admin

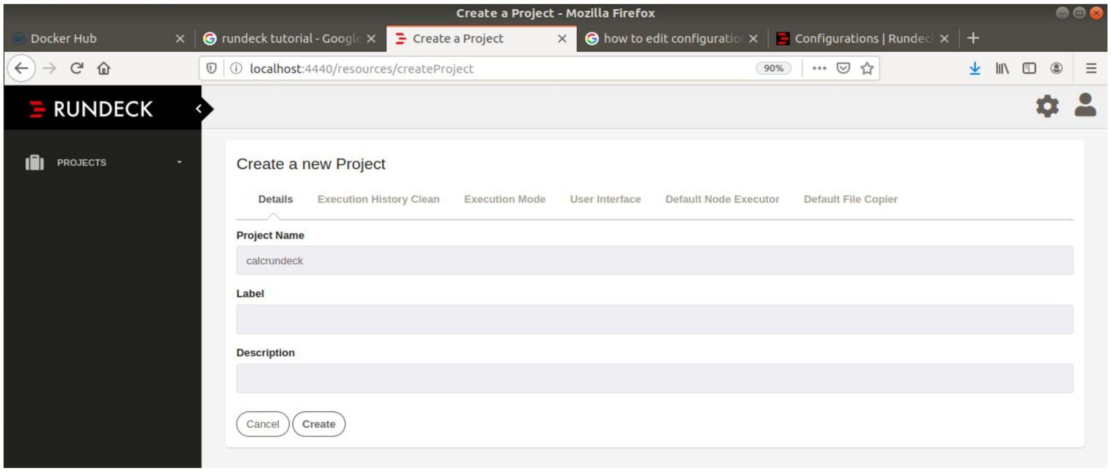
Key Storage provides a global directory-like structure to save Public and Private Keys and Passwords, for use with Node Execution authentication.

© Copyright 2020 Rundeck, Inc. All rights reserved.

- Create a rundeck project.

  Create new project in rundeck. Add name(say **calcrundeck**) under Details tab. Add SSH storage path(i.e key path) and SSH authentication password(i.e key password) under the Default Node Executor and Default Node Copier tab. Click on create.

  Created projects can be seen under the projects dropdown on the left side.

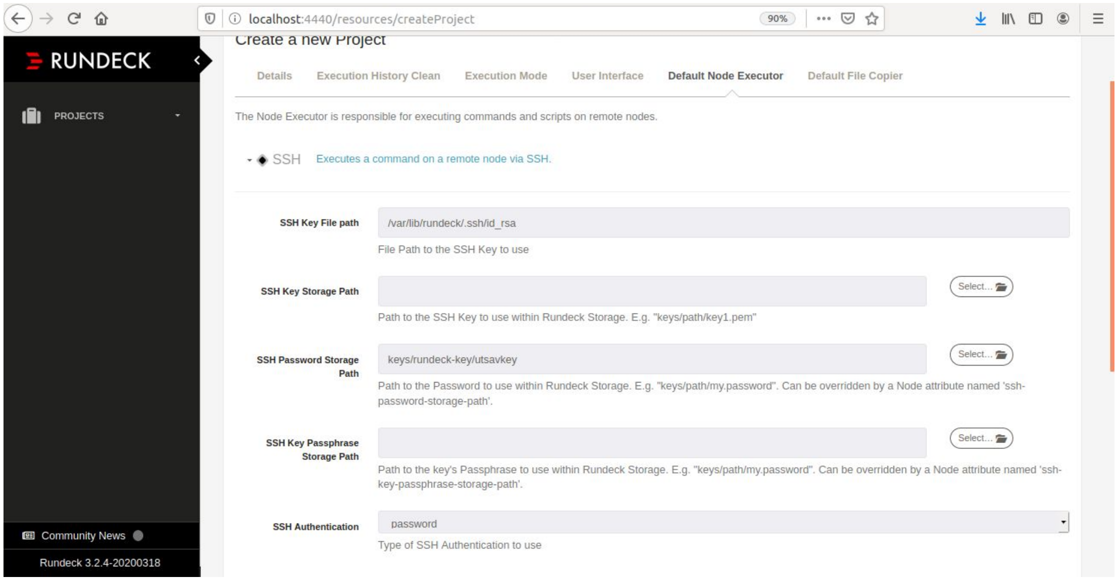


Create a new Project

Project Name: calcrundeck

Label:

Description:



Create a new Project

The Node Executor is responsible for executing commands and scripts on remote nodes.

SSH Executes a command on a remote node via SSH.

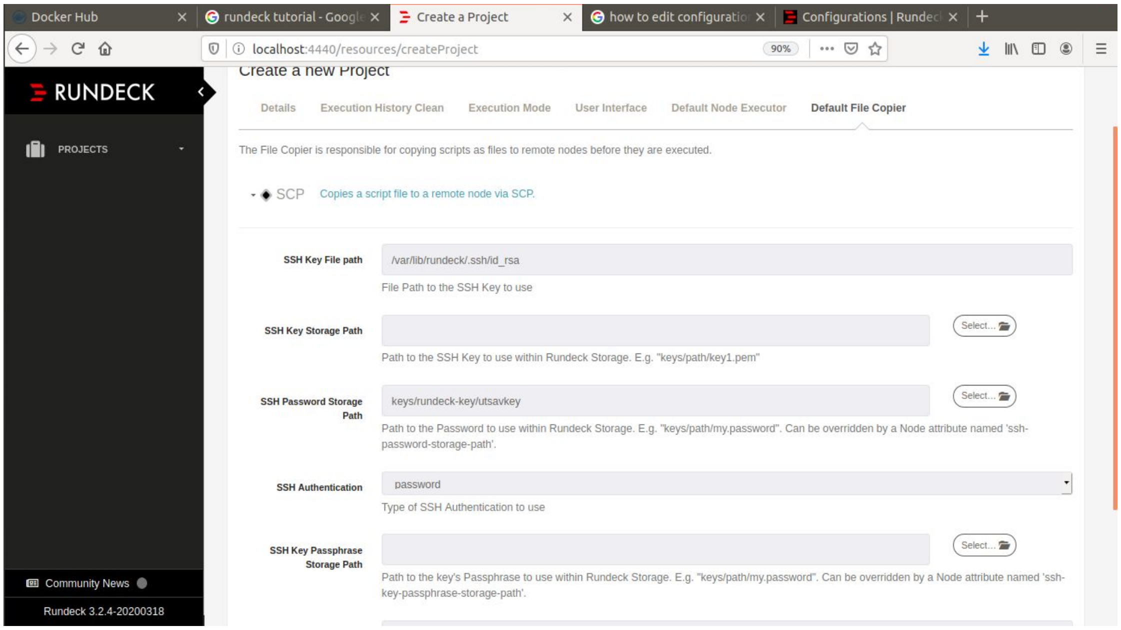
SSH Key File path: /var/lib/rundeck/.ssh/id_rsa
File Path to the SSH Key to use

SSH Key Storage Path:
Path to the SSH Key to use within Rundeck Storage. E.g. "keys/path/key1.pem"

SSH Password Storage Path: keys/rundeck-key/utsavkey
Path to the Password to use within Rundeck Storage. E.g. "keys/path/my.password". Can be overridden by a Node attribute named 'ssh-password-storage-path'.

SSH Key Passphrase Storage Path:
Path to the key's Passphrase to use within Rundeck Storage. E.g. "keys/path/my.password". Can be overridden by a Node attribute named 'ssh-key-passphrase-storage-path'.

SSH Authentication: password
Type of SSH Authentication to use



Create a new Project

The File Copier is responsible for copying scripts as files to remote nodes before they are executed.

SCP Copies a script file to a remote node via SCP.

SSH Key File path: /var/lib/rundeck/.ssh/id_rsa
File Path to the SSH Key to use

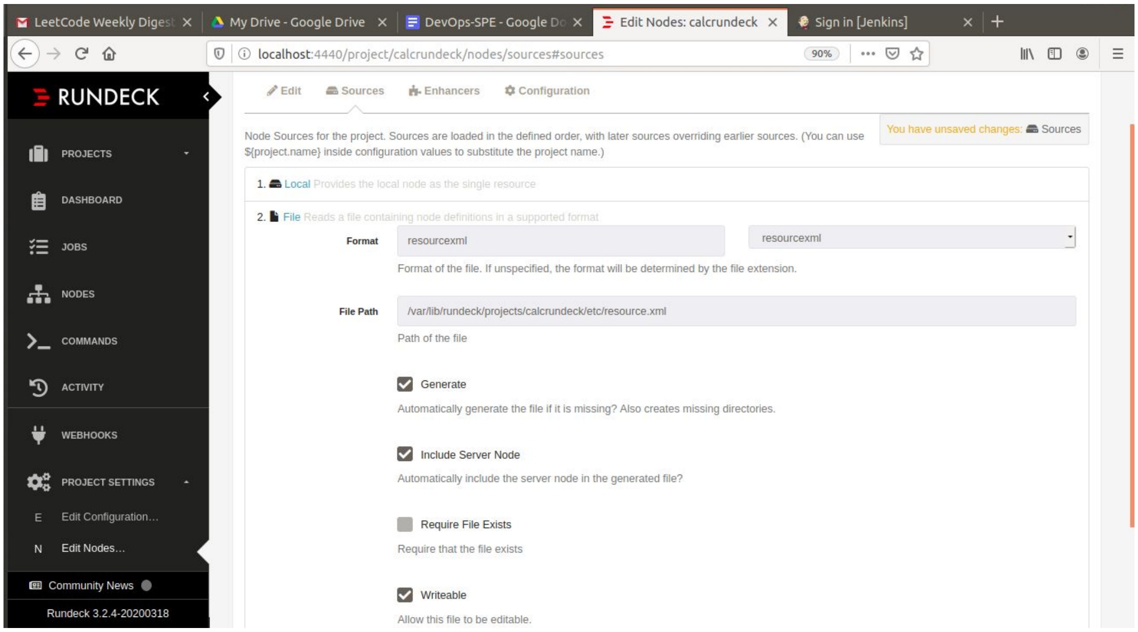
SSH Key Storage Path:
Path to the SSH Key to use within Rundeck Storage. E.g. "keys/path/key1.pem"

SSH Password Storage Path: keys/rundeck-key/utsavkey
Path to the Password to use within Rundeck Storage. E.g. "keys/path/my.password". Can be overridden by a Node attribute named 'ssh-password-storage-path'.

SSH Authentication: password
Type of SSH Authentication to use

SSH Key Passphrase Storage Path:
Path to the key's Passphrase to use within Rundeck Storage. E.g. "keys/path/my.password". Can be overridden by a Node attribute named 'ssh-key-passphrase-storage-path'.

- Create a node inside the above created rundeck project.
  Select your project from the left side. Goto project settings->Edit Nodes→Add a new node source -> Select File. Under Sources Tab:
  1) select format as resourcexml.
  2) provide the file path as /var/lib/rundeck/projects/<**project_name**>/etc/resource.xml.
  3) select all checkbox except Require file exists
  Click on Save.



You have unsaved changes: Sources

Node Sources for the project. Sources are loaded in the defined order, with later sources overriding earlier sources. (You can use ${project.name} inside configuration values to substitute the project name.)

1. Local Provides the local node as the single resource

2. File Reads a file containing node definitions in a supported format

Format: resourcexml | resourcexml

Format of the file. If unspecified, the format will be determined by the file extension.

File Path: /var/lib/rundeck/projects/calcrundeck/etc/resource.xml

Path of the file

☑ Generate

Automatically generate the file if it is missing? Also creates missing directories.

☑ Include Server Node

Automatically include the server node in the generated file?

☐ Require File Exists

Require that the file exists

☑ Writeable

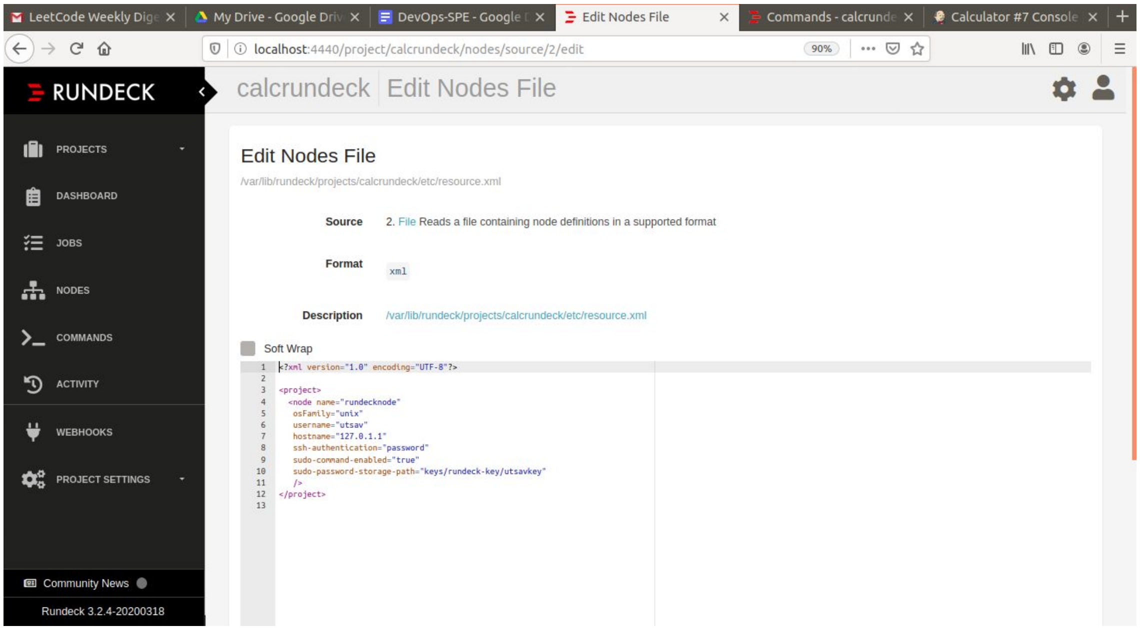
Allow this file to be editable.

Goto Project Setting -> Edit Nodes -> Modify the above created node and update the node details as following.

```
<project>
        <node name=<any node name>
          osFamily="unix"
          username=<node username>
          hostname=<node IP>
          ssh-authentication="password"
          sudo-command-enabled="true"
          sudo-password-storage-path=<path of the key>
          />
</project>
```

Click on Save.

Below is a screenshot of the configured details as mentioned above.



Edit Nodes File

/var/lib/rundeck/projects/calcrundeck/etc/resource.xml

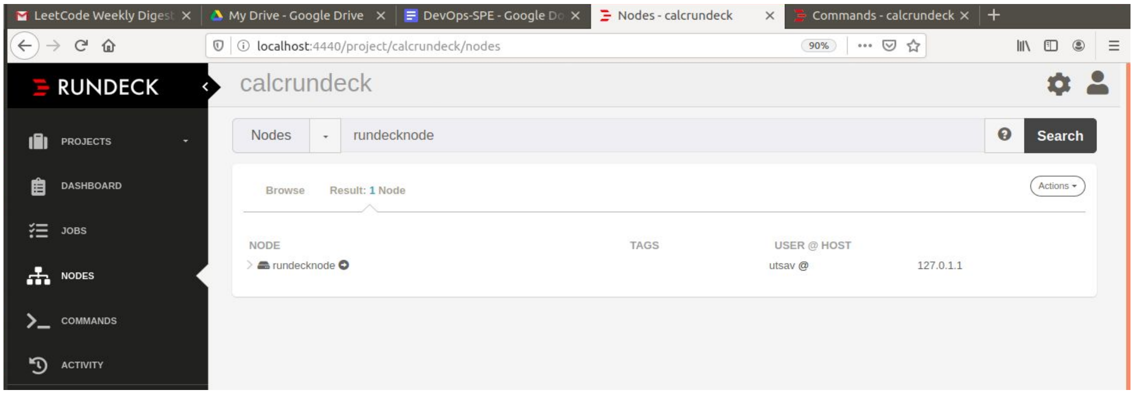
Source: 2. File Reads a file containing node definitions in a supported format

Format: xml

Description: /var/lib/rundeck/projects/calcrundeck/etc/resource.xml

```
<?xml version="1.0" encoding="UTF-8"?>

<project>
  <node name="rundecknode"
   osFamily="unix"
   username="utsav"
   hostname="127.0.1.1"
   ssh-authentication="password"
   sudo-command-enabled="true"
   sudo-password-storage-path="keys/rundeck-key/utsavkey"
   />
</project>
```

Created node can be seen under nodes when searched as shown below.

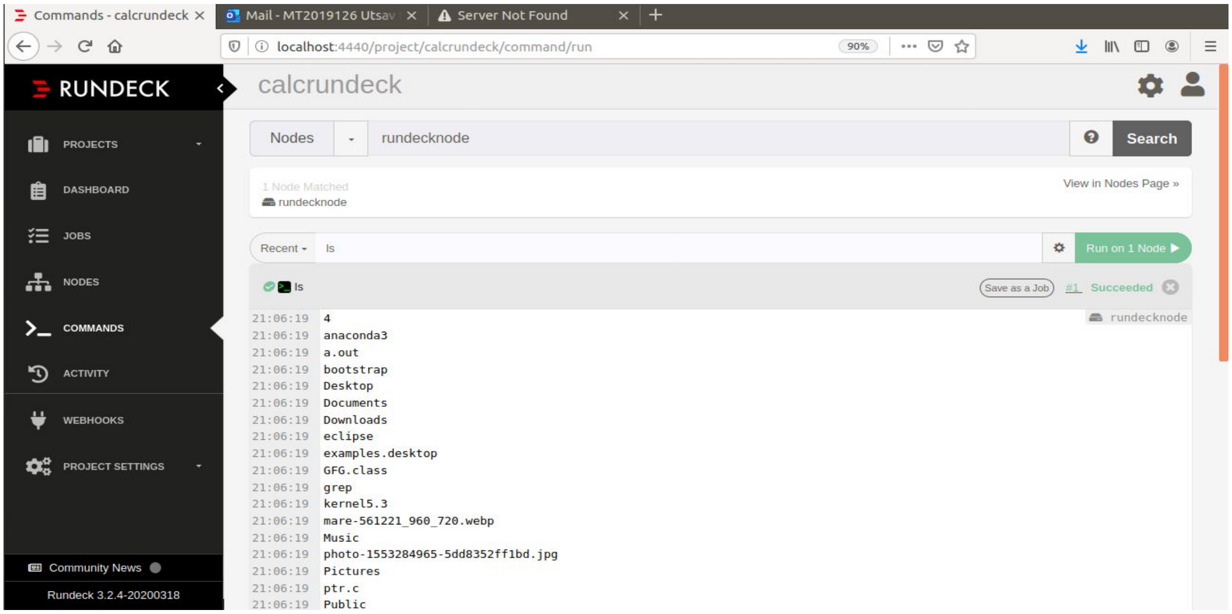


NODE	TAGS	USER @ HOST	
rundecknode		utsav @	127.0.1.1

- To connect to the node via ssh we need to enable ssh in the node.
  Run following command in the node terminal to enable the ssh.
  service ssh start

  If ssh is not installed in the node. Use the below commands to install them.
  apt-get update
  apt-get upgrade
  apt-get install openssh-server

- Run some action in node from the rundeck to verify whether the connection is working or not.
  Goto Projects -> Commands -> Select the node by searching -> Run command ls.



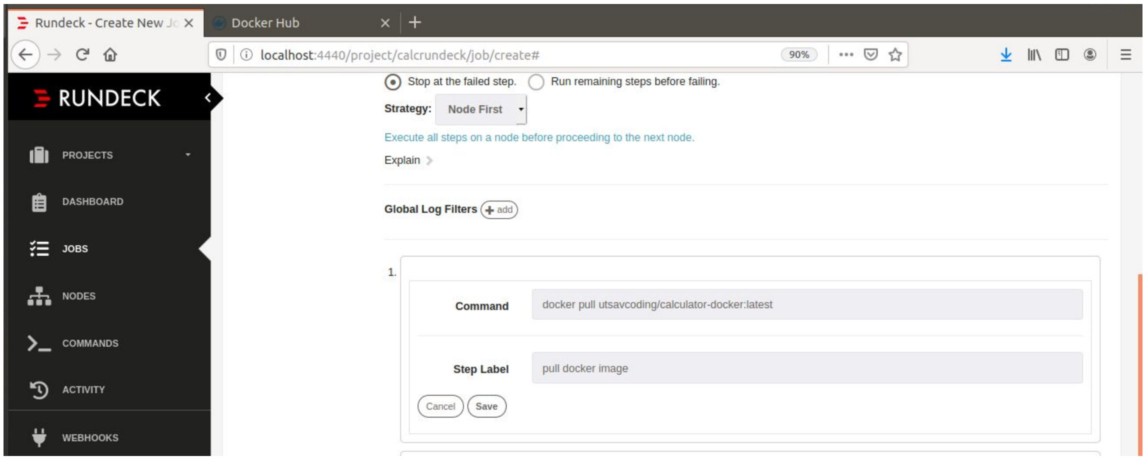
Nodes: rundecknode

1 Node Matched
rundecknode

ls

```
21:06:19  4
21:06:19  anaconda3
21:06:19  a.out
21:06:19  bootstrap
21:06:19  Desktop
21:06:19  Documents
21:06:19  Downloads
21:06:19  eclipse
21:06:19  examples.desktop
21:06:19  GFG.class
21:06:19  grep
21:06:19  kernel5.3
21:06:19  mare-561221_960_720.webp
21:06:19  Music
21:06:19  photo-1553284965-5dd8352ff1bd.jpg
21:06:19  Pictures
21:06:19  ptr.c
21:06:19  Public
```

- Create a job under the project which will be triggered from jenkins.
  Goto Jobs-> Job Actions -> New Jobs. Mention the job name under Details tab. Under Workflow tab, choose command.
  Add two commands as shown below for the docker:-
  1) Fetch docker image from docker hu
     docker pull <**dockerhub-username**>/<**dockerhubimage**>:latest
  2) Run container from the image and publish the URL
     docker run -d -p 8080:8080 <**dockerhub-username**>/<**dockerhubimage**>:latest



● Stop at the failed step. ○ Run remaining steps before failing.

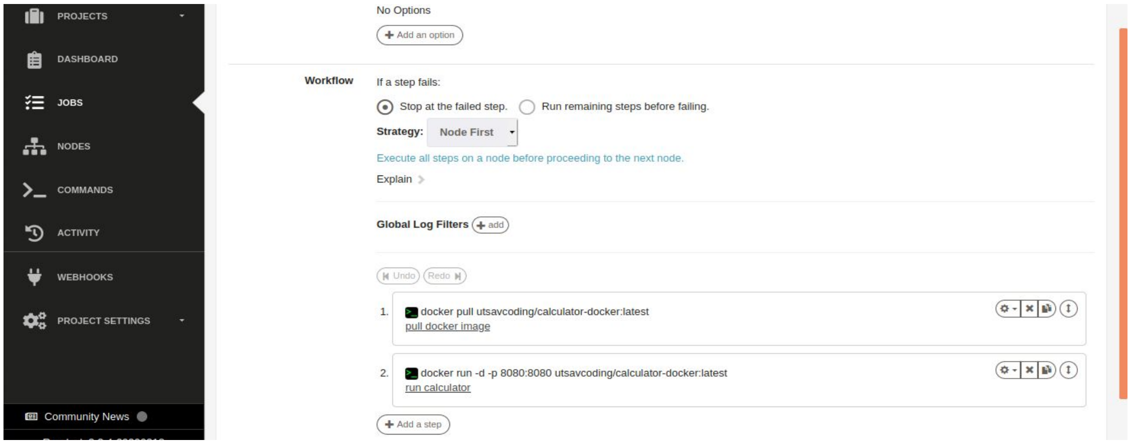
Strategy: Node First

Execute all steps on a node before proceeding to the next node.

1.

Command: docker pull utsavcoding/calculator-docker:latest

Step Label: pull docker image



No Options

Workflow

If a step fails:

● Stop at the failed step. ○ Run remaining steps before failing.

Strategy: Node First

Execute all steps on a node before proceeding to the next node.

Explain

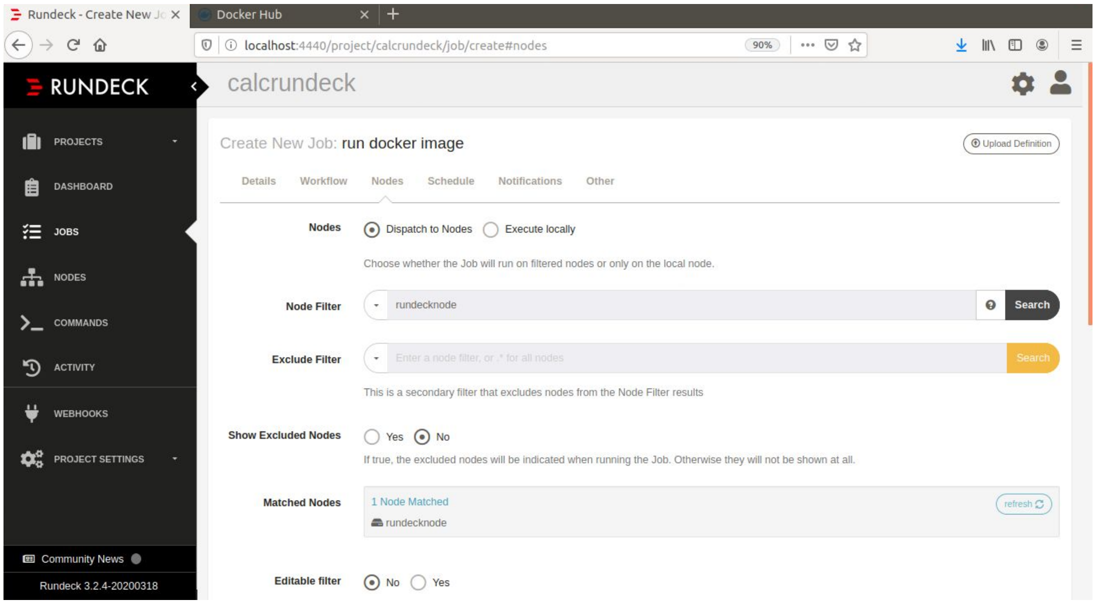
Global Log Filters

1. docker pull utsavcoding/calculator-docker:latest
pull docker image

2. docker run -d -p 8080:8080 utsavcoding/calculator-docker:latest
run calculator

After the above is done. Under Nodes tab, link the job to the configured node, where job will be executed.

Select Dispatch to Nodes. Give your name under Node Filter. Click on Save.



localhost:4440/project/calcrundeck/job/create#nodes

calcrundeck

Create New Job: run docker image

Nodes ● Dispatch to Nodes ○ Execute locally

Choose whether the Job will run on filtered nodes or only on the local node.

Node Filter: rundecknode

Exclude Filter: Enter a node filter, or .* for all nodes

This is a secondary filter that excludes nodes from the Node Filter results

Show Excluded Nodes ○ Yes ● No

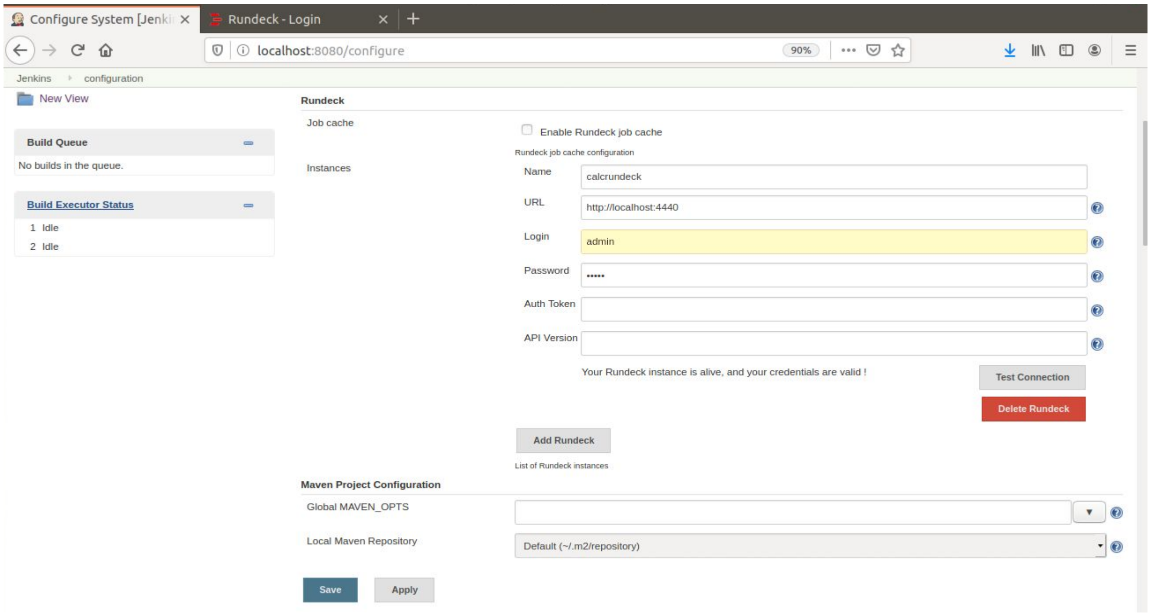
If true, the excluded nodes will be indicated when running the Job. Otherwise they will not be shown at all.

Matched Nodes: 1 Node Matched
rundecknode

Editable filter ● No ○ Yes

4. Jenkins:

- Install jenkins, and change the port number of jenkins to 8081(to avoid conflict with tomcat).
  First, add the repository key to the system:
  $ wget -q -O - http://pkg.jenkins-ci.org/debian/jenkins-ci.org.key | sudo apt-key add -
  append the Debian package repository address to the server's sources.list:
  $ sudo sh -c 'echo deb http://pkg.jenkins-ci.org/debian-stable binary/ > /etc/apt/sources.list.d/jenkins.list'
  $ sudo apt update
  $ sudo apt install jenkins
- Start Jenkins
  $ sudo systemctl start jenkins
- Unlock jenkins -To get the password use the following command.
  $ sudo cat /var/lib/jenkins/secrets/initialAdminPassword
- Now create a user, and jenkins is ready to be used.
- Check http://localhost:8081/
- Install following plugins in the jenkins-
  - ➢ Git
  - ➢ Maven
  - ➢ Pipeline
  - ➢ Rundeck
  - ➢ Docker
- Go to Manage Jenkins -> Configure System
  Configure rundeck. Mention your rundeck project name, user id and password.



Rundeck

Job cache: ☐ Enable Rundeck job cache

Rundeck job cache configuration

Instances

Name: calcrundeck

URL: http://localhost:4440

Login: admin

Password: •••••

Auth Token:

API Version:

Your Rundeck instance is alive, and your credentials are valid !

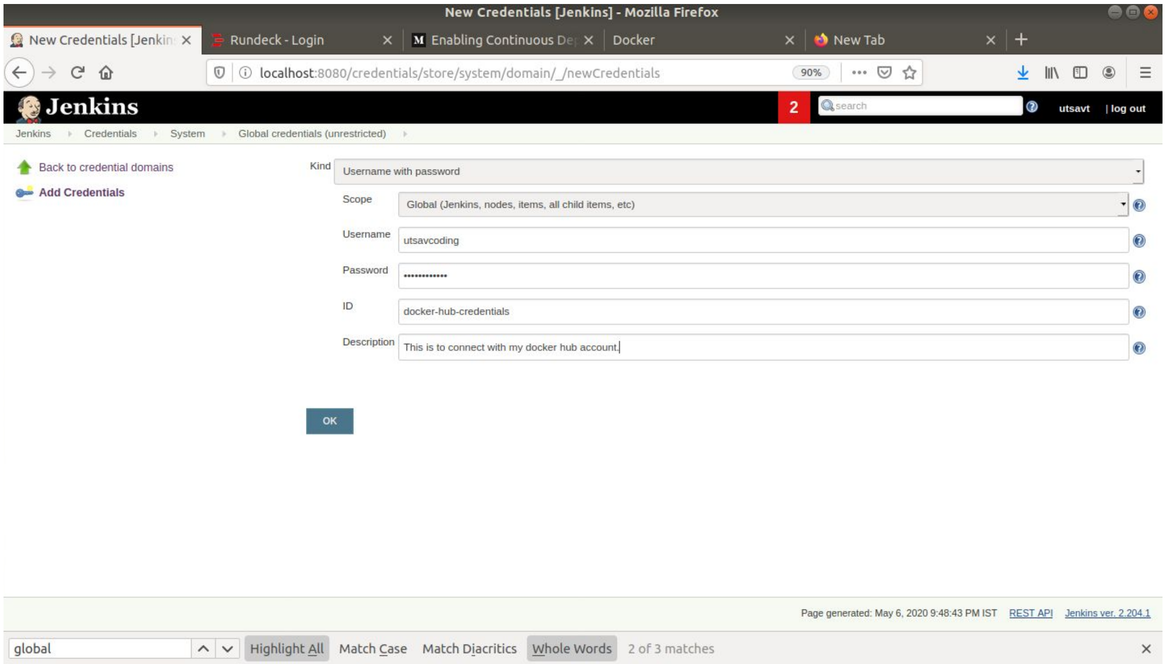
List of Rundeck instances

Maven Project Configuration

Global MAVEN_OPTS:

Local Maven Repository: Default (~/.m2/repository)

- Need to configure docker hub credential as global credential for jenkins. Goto Credentials->Goto system. Click on Global Credentials. Then Add Credentials. Mention the credential details of docker hub account. Also mention a ID for the credential(remember this ID, as this will be used during pipeline creation later on). Below is a screenshot of the mentioned details.



Kind: Username with password

Scope: Global (Jenkins, nodes, items, all child items, etc)

Username: utsavcoding

Password: ••••••••••••

ID: docker-hub-credentials

Description: This is to connect with my docker hub account.

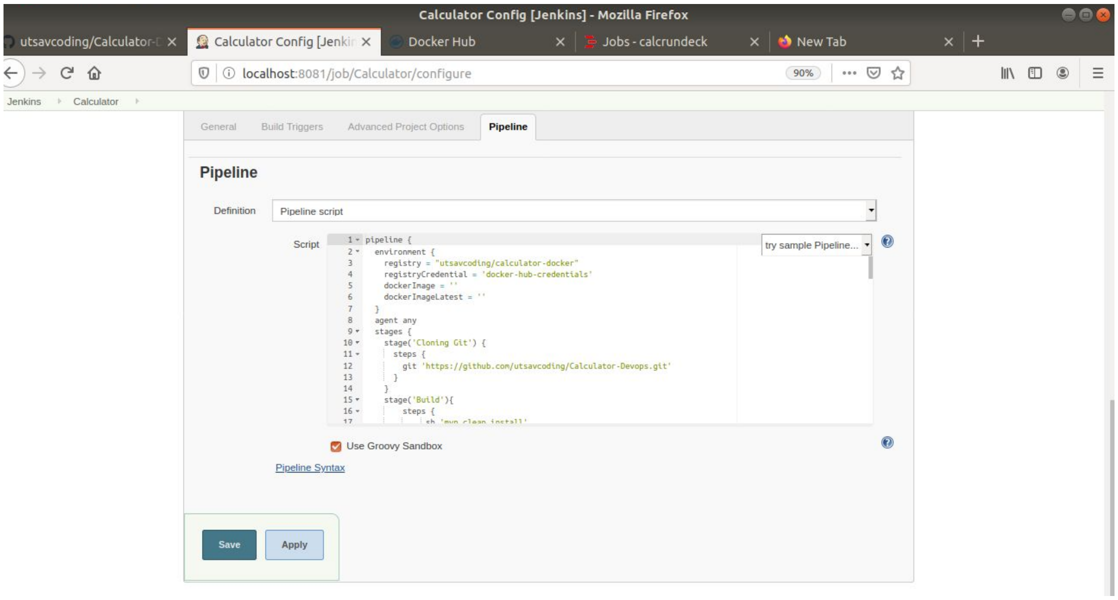
Page generated: May 6, 2020 9:48:43 PM IST

- Create a new pipeline in jenkins to trigger the entire process of CI & CD. Write a project pipeline script as following:-

```
pipeline {
 environment {
        registry = <dockerhub-username>/<dockerhubimage>
        registryCredential = <ID mentioned in the global credential in jenkins>
        dockerImage = ''
        dockerImageLatest = ''
 }
 agent any
 stages {
        stage('Cloning Git') {
        steps {
        git '<github repo link>'
        }
        }
        stage('Build'){
        steps {
        sh 'mvn clean install'
        }
        }
        stage('Test'){
        steps {
        sh 'mvn test'
        }
        }
        stage('Building image') {
        steps{
        script {
        dockerImage = docker.build registry + ":$BUILD_NUMBER"
        dockerImageLatest = docker.build registry + ":latest"
        }
        }
        }
        stage('Deploy Image') {
        steps{
        script {
        docker.withRegistry( '', registryCredential ) {
        dockerImage.push()
        dockerImageLatest.push()
        }
        }
        }
        }
        stage('Remove Unused docker image') {
        steps{
        sh "docker rmi $registry:$BUILD_NUMBER"
        }
        }
        stage('Execute Rundeck job') {
        steps {
        script {
        step([$class: "RundeckNotifier",
        includeRundeckLogs: true,
        jobId: <job Id of the rundeck job> ,
        rundeckInstance: <rundeck project name>,
        shouldFailTheBuild: true,
        shouldWaitForRundeckJob: true,
        tailLog: true])
        }
        }
        }
 }
}
```

Here is the link to the jenkins pipeline script used for this calculator project configuration on my github repo: https://github.com/utsavcoding/Calculator-Devops/blob/master/PipelineJenkins

Go to New item -> Pipeline. Give a name to the pipeline.
Add the above script under script section as shown below. Click on Save.



Pipeline

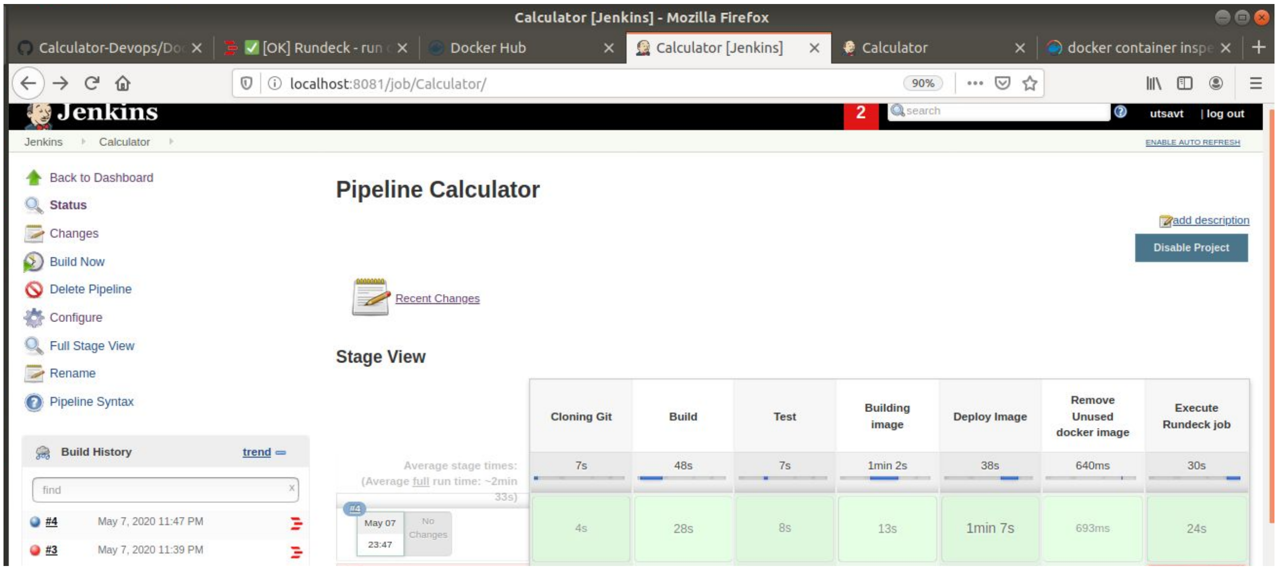
Definition: Pipeline script

Script

```
pipeline {
  environment {
    registry = "utsavcoding/calculator-docker"
    registryCredential = 'docker-hub-credentials'
    dockerImage = ''
    dockerImageLatest = ''
  }
  agent any
  stages {
    stage('Cloning Git') {
      steps {
        git 'https://github.com/utsavcoding/Calculator-Devops.git'
      }
    }
    stage('Build'){
        steps {
            sh 'mvn clean install'
```

☑ Use Groovy Sandbox

- Run the pipeline from the jenkins dashboard. On success, all the stages will be green as shown below.



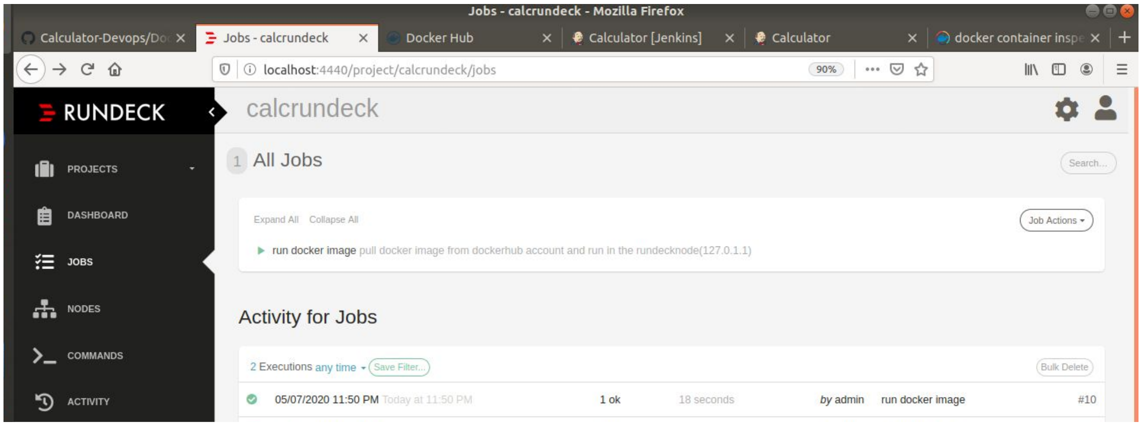
Pipeline Calculator

Stage View

	Cloning Git	Build	Test	Building image	Deploy Image	Remove Unused docker image	Execute Rundeck job
Average stage times: (Average full run time: ~2min 33s)	7s	48s	7s	1min 2s	38s	640ms	30s
#4 May 07 23:47 No Changes	4s	28s	8s	13s	1min 7s	693ms	24s

#4	May 7, 2020 11:47 PM
#3	May 7, 2020 11:39 PM

- Check rundeck under the jobs to see its status.



calcrundeck

1 All Jobs

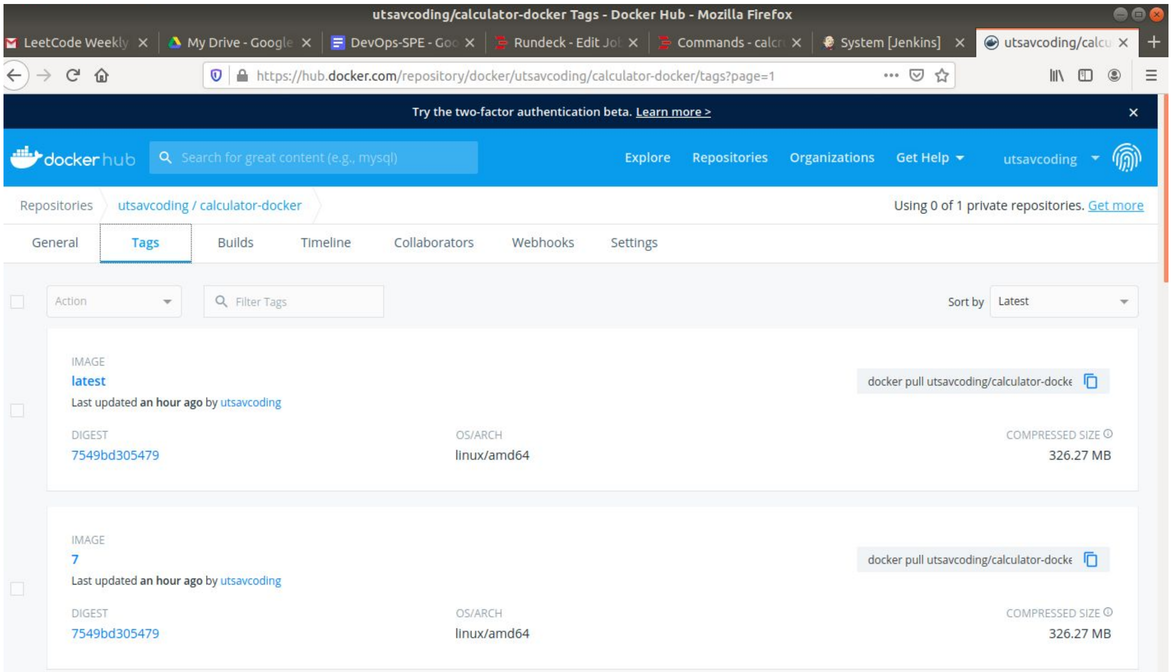
▶ run docker image pull docker image from dockerhub account and run in the rundecknode(127.0.1.1)

Activity for Jobs

2 Executions any time

✓ 05/07/2020 11:50 PM Today at 11:50 PM 1 ok 18 seconds *by* admin run docker image #10

- Check docker hub account.



Try the two-factor authentication beta. Learn more >

Using 0 of 1 private repositories. Get more

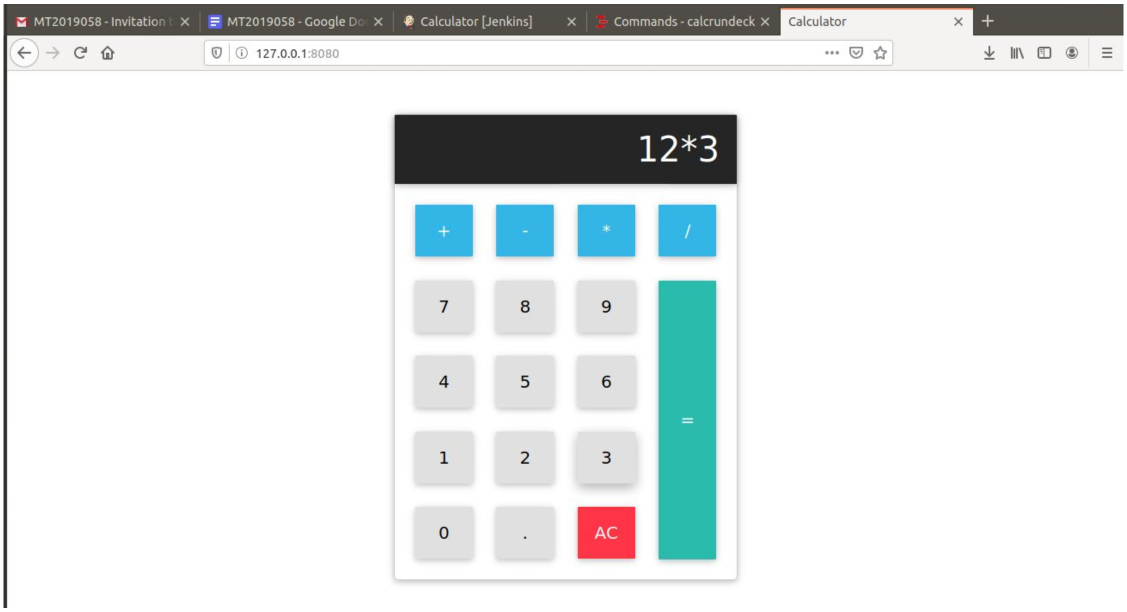
IMAGE
latest
Last updated **an hour ago** by utsavcoding
docker pull utsavcoding/calculator-docke

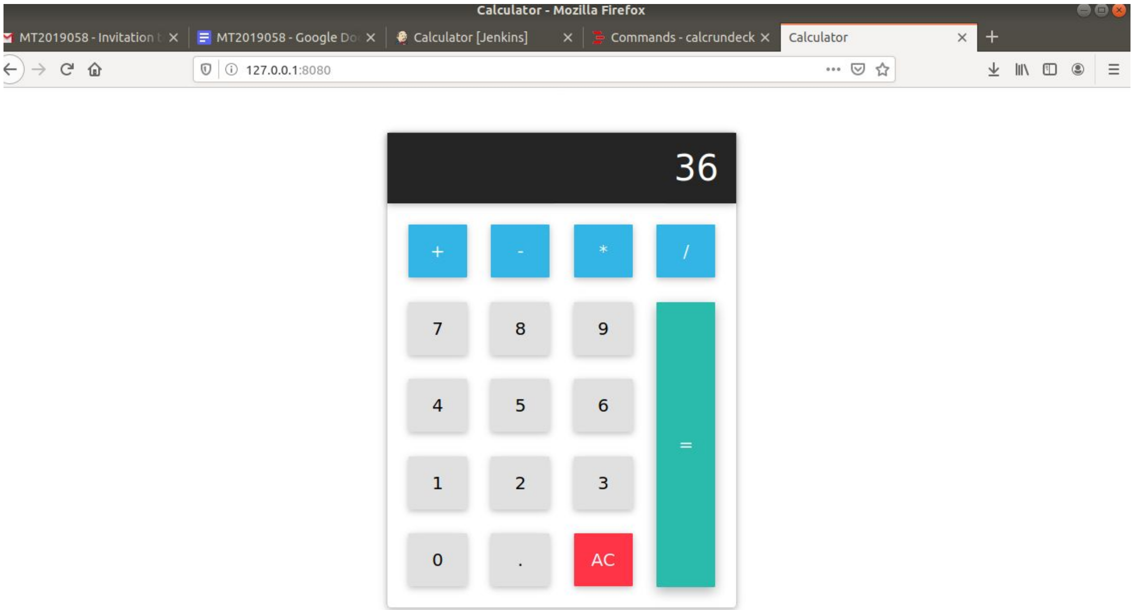
DIGEST	OS/ARCH	COMPRESSED SIZE
7549bd305479	linux/amd64	326.27 MB

IMAGE
7
Last updated **an hour ago** by utsavcoding
docker pull utsavcoding/calculator-docke

DIGEST	OS/ARCH	COMPRESSED SIZE
7549bd305479	linux/amd64	326.27 MB

- Type exposed URL in host to check out the application.
  Check http://127.0.0.1:8080/

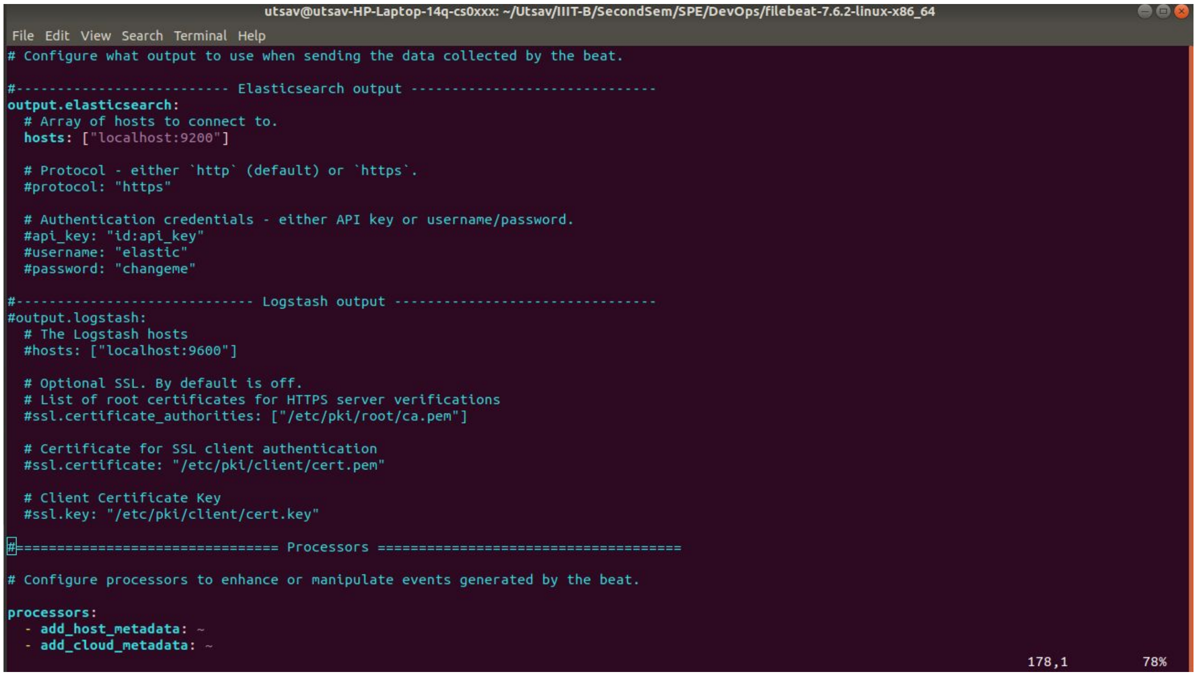




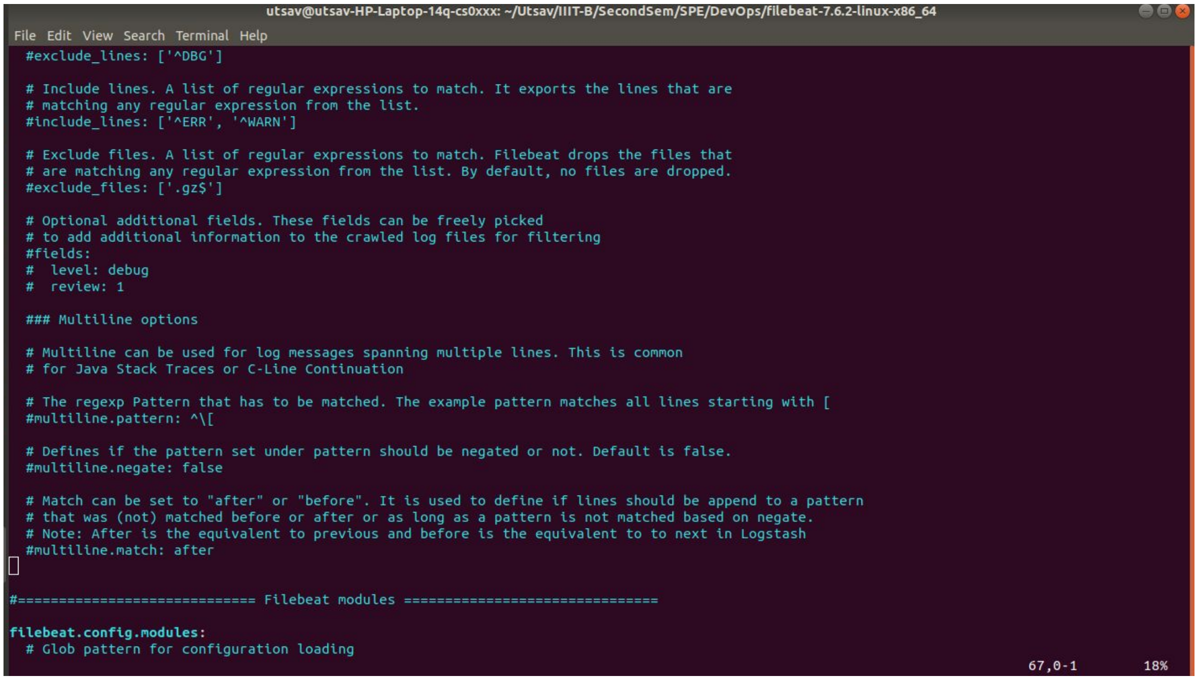
5. ELK:

- Download ElasticSearch , Filebeat and Kibana from https://www.elastic.co/downloads/ in host node.
- Configure filebeat.yml in the filebeat folder to take input from docker container logs and visualize them in kibana

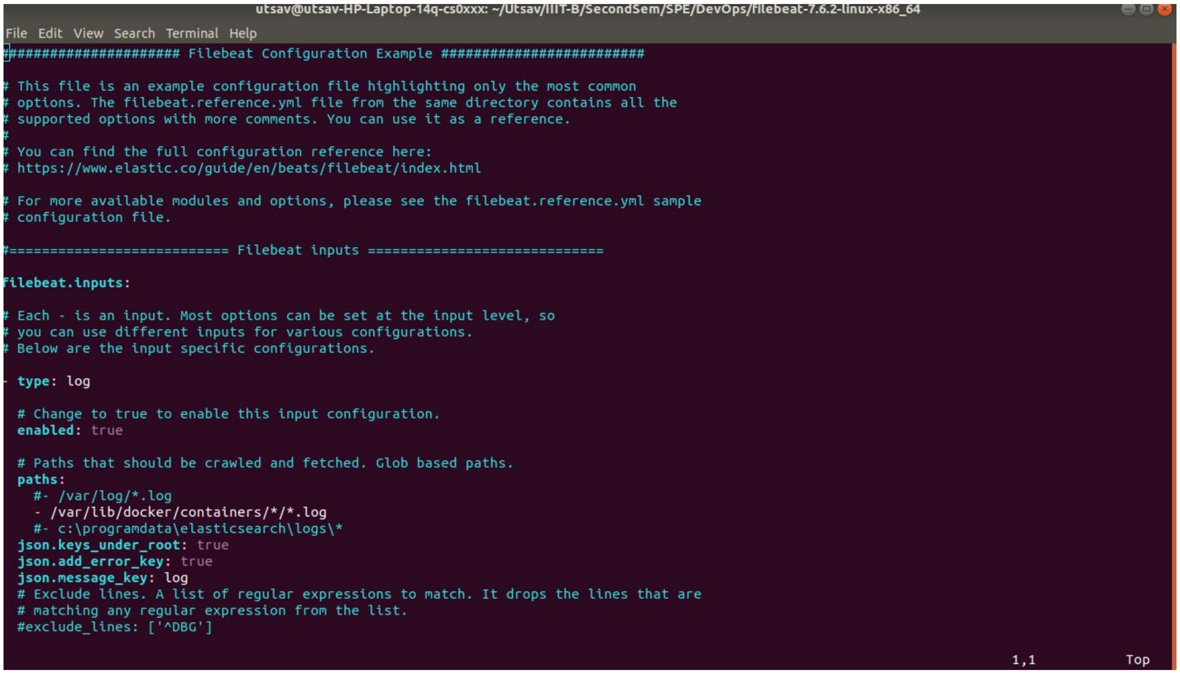
Below is a screenshot of configured filebeat.yml file.


utsav@utsav-HP-Laptop-14q-cs0xxx: ~/Utsav/IIIT-B/SecondSem/SPE/DevOps/filebeat-7.6.2-linux-x86_64
File Edit View Search Terminal Help

```
# Configure what output to use when sending the data collected by the beat.

#-------------------------- Elasticsearch output ------------------------------
output.elasticsearch:
  # Array of hosts to connect to.
  hosts: ["localhost:9200"]

  # Protocol - either `http` (default) or `https`.
  #protocol: "https"

  # Authentication credentials - either API key or username/password.
  #api_key: "id:api_key"
  #username: "elastic"
  #password: "changeme"

#----------------------------- Logstash output --------------------------------
#output.logstash:
  # The Logstash hosts
  #hosts: ["localhost:9600"]

  # Optional SSL. By default is off.
  # List of root certificates for HTTPS server verifications
  #ssl.certificate_authorities: ["/etc/pki/root/ca.pem"]

  # Certificate for SSL client authentication
  #ssl.certificate: "/etc/pki/client/cert.pem"

  # Client Certificate Key
  #ssl.key: "/etc/pki/client/cert.key"

#================================ Processors =====================================

# Configure processors to enhance or manipulate events generated by the beat.

processors:
  - add_host_metadata: ~
  - add_cloud_metadata: ~
                                                                  178,1         78%
```

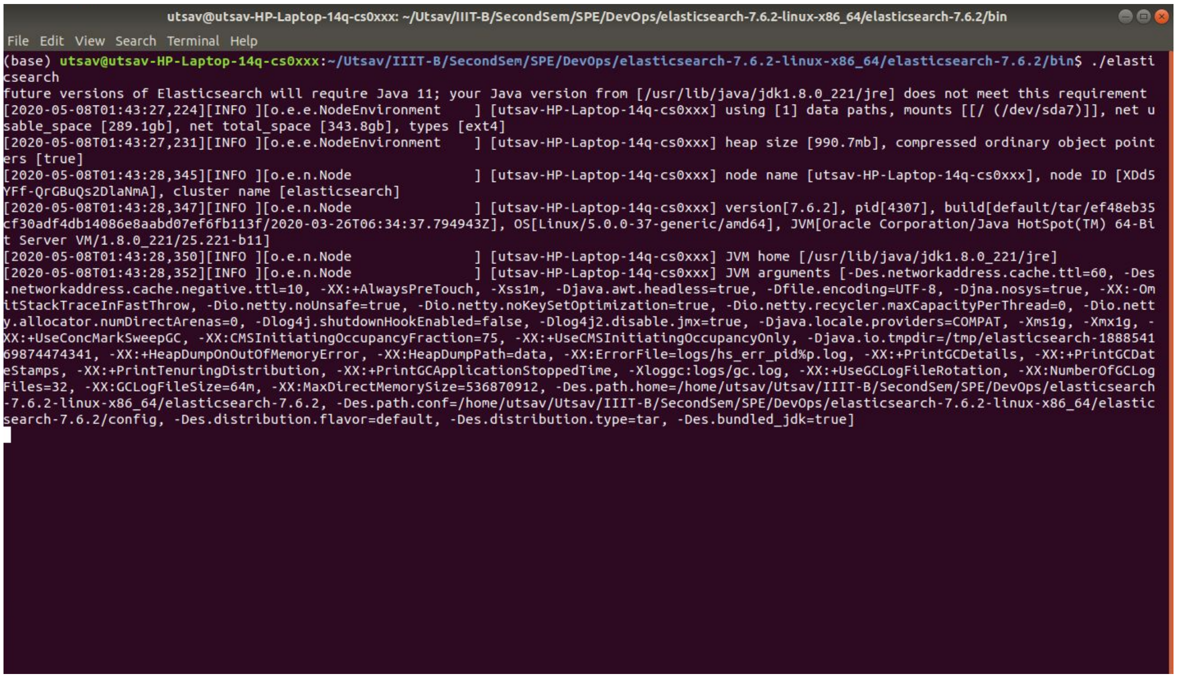

utsav@utsav-HP-Laptop-14q-cs0xxx: ~/Utsav/IIIT-B/SecondSem/SPE/DevOps/filebeat-7.6.2-linux-x86_64
File Edit View Search Terminal Help

```
  #exclude_lines: ['^DBG']

  # Include lines. A list of regular expressions to match. It exports the lines that are
  # matching any regular expression from the list.
  #include_lines: ['^ERR', '^WARN']

  # Exclude files. A list of regular expressions to match. Filebeat drops the files that
  # are matching any regular expression from the list. By default, no files are dropped.
  #exclude_files: ['.gz$']

  # Optional additional fields. These fields can be freely picked
  # to add additional information to the crawled log files for filtering
  #fields:
  #  level: debug
  #  review: 1

  ### Multiline options

  # Multiline can be used for log messages spanning multiple lines. This is common
  # for Java Stack Traces or C-Line Continuation

  # The regexp Pattern that has to be matched. The example pattern matches all lines starting with [
  #multiline.pattern: ^\[

  # Defines if the pattern set under pattern should be negated or not. Default is false.
  #multiline.negate: false

  # Match can be set to "after" or "before". It is used to define if lines should be append to a pattern
  # that was (not) matched before or after or as long as a pattern is not matched based on negate.
  # Note: After is the equivalent to previous and before is the equivalent to to next in Logstash
  #multiline.match: after


#============================= Filebeat modules ===============================

filebeat.config.modules:
  # Glob pattern for configuration loading
                                                                  67,0-1        18%
```


utsav@utsav-HP-Laptop-14q-cs0xxx: ~/Utsav/IIIT-B/SecondSem/SPE/DevOps/filebeat-7.6.2-linux-x86_64
File Edit View Search Terminal Help

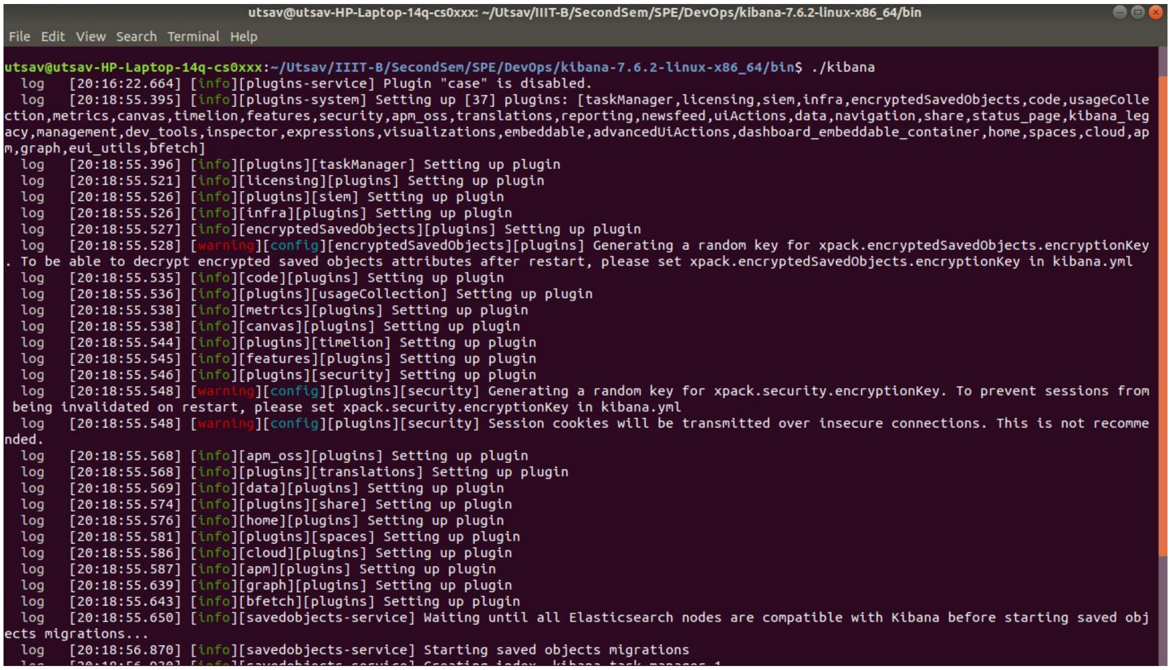
```
###################### Filebeat Configuration Example #########################

# This file is an example configuration file highlighting only the most common
# options. The filebeat.reference.yml file from the same directory contains all the
# supported options with more comments. You can use it as a reference.
#
# You can find the full configuration reference here:
# https://www.elastic.co/guide/en/beats/filebeat/index.html

# For more available modules and options, please see the filebeat.reference.yml sample
# configuration file.

#=========================== Filebeat inputs =============================

filebeat.inputs:

# Each - is an input. Most options can be set at the input level, so
# you can use different inputs for various configurations.
# Below are the input specific configurations.

- type: log

  # Change to true to enable this input configuration.
  enabled: true

  # Paths that should be crawled and fetched. Glob based paths.
  paths:
    #- /var/log/*.log
    - /var/lib/docker/containers/*/*.log
    #- c:\programdata\elasticsearch\logs\*
  json.keys_under_root: true
  json.add_error_key: true
  json.message_key: log
  # Exclude lines. A list of regular expressions to match. It drops the lines that are
  # matching any regular expression from the list.
  #exclude_lines: ['^DBG']

                                                                  1,1           Top
```

- Start the elasticsearch, kibana and filebeat from terminal in this order.
- Start the elasticsearch-
  Go to the bin folder and run **./elasticsearch**


utsav@utsav-HP-Laptop-14q-cs0xxx: ~/Utsav/IIIT-B/SecondSem/SPE/DevOps/elasticsearch-7.6.2-linux-x86_64/elasticsearch-7.6.2/bin
File Edit View Search Terminal Help

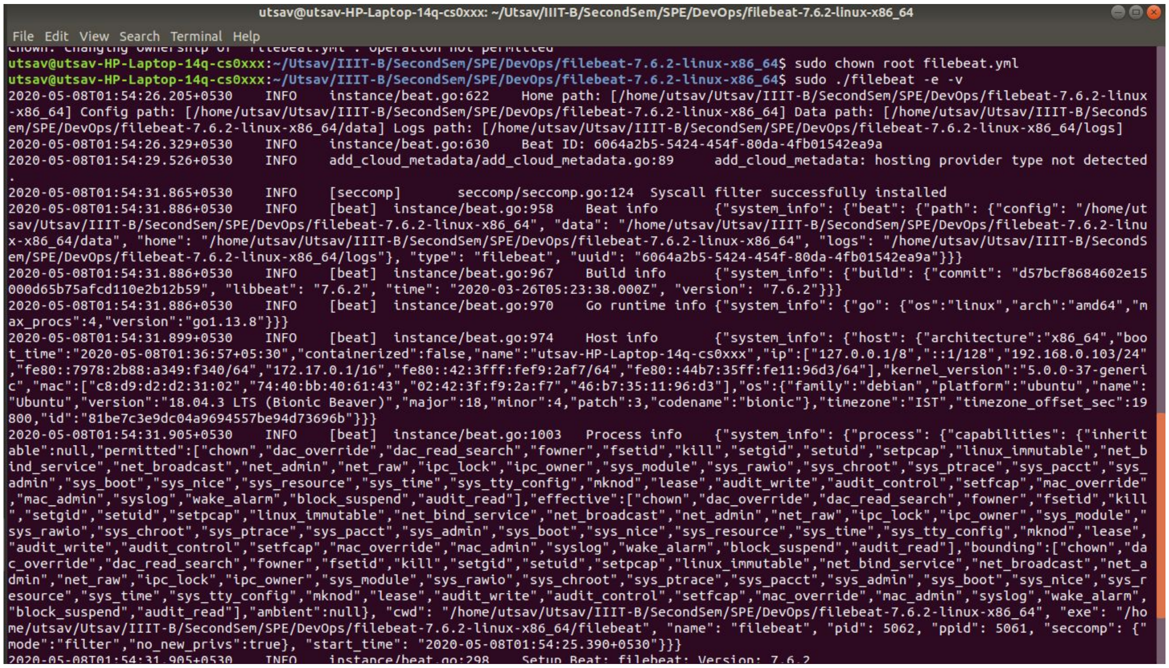
```
(base) utsav@utsav-HP-Laptop-14q-cs0xxx:~/Utsav/IIIT-B/SecondSem/SPE/DevOps/elasticsearch-7.6.2-linux-x86_64/elasticsearch-7.6.2/bin$ ./elasti
csearch
future versions of Elasticsearch will require Java 11; your Java version from [/usr/lib/java/jdk1.8.0_221/jre] does not meet this requirement
[2020-05-08T01:43:27,224][INFO ][o.e.e.NodeEnvironment    ] [utsav-HP-Laptop-14q-cs0xxx] using [1] data paths, mounts [[/ (/dev/sda7)]], net u
sable_space [289.1gb], net total_space [343.8gb], types [ext4]
[2020-05-08T01:43:27,231][INFO ][o.e.e.NodeEnvironment    ] [utsav-HP-Laptop-14q-cs0xxx] heap size [990.7mb], compressed ordinary object point
ers [true]
[2020-05-08T01:43:28,345][INFO ][o.e.n.Node               ] [utsav-HP-Laptop-14q-cs0xxx] node name [utsav-HP-Laptop-14q-cs0xxx], node ID [XDd5
YFf-QrGBuQs2DlaNmA], cluster name [elasticsearch]
[2020-05-08T01:43:28,347][INFO ][o.e.n.Node               ] [utsav-HP-Laptop-14q-cs0xxx] version[7.6.2], pid[4307], build[default/tar/ef48eb35
cf30adf4db14086e8aabd07ef6fb113f/2020-03-26T06:34:37.794943Z], OS[Linux/5.0.0-37-generic/amd64], JVM[Oracle Corporation/Java HotSpot(TM) 64-Bi
t Server VM/1.8.0_221/25.221-b11]
[2020-05-08T01:43:28,350][INFO ][o.e.n.Node               ] [utsav-HP-Laptop-14q-cs0xxx] JVM home [/usr/lib/java/jdk1.8.0_221/jre]
[2020-05-08T01:43:28,352][INFO ][o.e.n.Node               ] [utsav-HP-Laptop-14q-cs0xxx] JVM arguments [-Des.networkaddress.cache.ttl=60, -Des
.networkaddress.cache.negative.ttl=10, -XX:+AlwaysPreTouch, -Xss1m, -Djava.awt.headless=true, -Dfile.encoding=UTF-8, -Djna.nosys=true, -XX:-Om
itStackTraceInFastThrow, -Dio.netty.noUnsafe=true, -Dio.netty.noKeySetOptimization=true, -Dio.netty.recycler.maxCapacityPerThread=0, -Dio.nett
y.allocator.numDirectArenas=0, -Dlog4j.shutdownHookEnabled=false, -Dlog4j2.disable.jmx=true, -Djava.locale.providers=COMPAT, -Xms1g, -Xmx1g, -
XX:+UseConcMarkSweepGC, -XX:CMSInitiatingOccupancyFraction=75, -XX:+UseCMSInitiatingOccupancyOnly, -Djava.io.tmpdir=/tmp/elasticsearch-1888541
69874474341, -XX:+HeapDumpOnOutOfMemoryError, -XX:HeapDumpPath=data, -XX:ErrorFile=logs/hs_err_pid%p.log, -XX:+PrintGCDetails, -XX:+PrintGCDat
eStamps, -XX:+PrintTenuringDistribution, -XX:+PrintGCApplicationStoppedTime, -Xloggc:logs/gc.log, -XX:+UseGCLogFileRotation, -XX:NumberOfGCLog
Files=32, -XX:GCLogFileSize=64m, -XX:MaxDirectMemorySize=536870912, -Des.path.home=/home/utsav/Utsav/IIIT-B/SecondSem/SPE/DevOps/elasticsearch
-7.6.2-linux-x86_64/elasticsearch-7.6.2, -Des.path.conf=/home/utsav/Utsav/IIIT-B/SecondSem/SPE/DevOps/elasticsearch-7.6.2-linux-x86_64/elastic
search-7.6.2/config, -Des.distribution.flavor=default, -Des.distribution.type=tar, -Des.bundled_jdk=true]
```

- Start the kibana-
  Go to the bin folder and run **./kibana**


utsav@utsav-HP-Laptop-14q-cs0xxx: ~/Utsav/IIIT-B/SecondSem/SPE/DevOps/kibana-7.6.2-linux-x86_64/bin
File Edit View Search Terminal Help

```
utsav@utsav-HP-Laptop-14q-cs0xxx:~/Utsav/IIIT-B/SecondSem/SPE/DevOps/kibana-7.6.2-linux-x86_64/bin$ ./kibana
  log   [20:16:22.664] [info][plugins-service] Plugin "case" is disabled.
  log   [20:18:55.395] [info][plugins-system] Setting up [37] plugins: [taskManager,licensing,siem,infra,encryptedSavedObjects,code,usageColle
ction,metrics,canvas,timelion,features,security,apm_oss,translations,reporting,newsfeed,uiActions,data,navigation,share,status_page,kibana_leg
acy,management,dev_tools,inspector,expressions,visualizations,embeddable,advancedUiActions,dashboard_embeddable_container,home,spaces,cloud,ap
m,graph,eui_utils,bfetch]
  log   [20:18:55.396] [info][plugins][taskManager] Setting up plugin
  log   [20:18:55.521] [info][licensing][plugins] Setting up plugin
  log   [20:18:55.526] [info][plugins][siem] Setting up plugin
  log   [20:18:55.526] [info][infra][plugins] Setting up plugin
  log   [20:18:55.527] [info][encryptedSavedObjects][plugins] Setting up plugin
  log   [20:18:55.528] [warning][config][encryptedSavedObjects][plugins] Generating a random key for xpack.encryptedSavedObjects.encryptionKey
. To be able to decrypt encrypted saved objects attributes after restart, please set xpack.encryptedSavedObjects.encryptionKey in kibana.yml
  log   [20:18:55.535] [info][code][plugins] Setting up plugin
  log   [20:18:55.536] [info][plugins][usageCollection] Setting up plugin
  log   [20:18:55.538] [info][metrics][plugins] Setting up plugin
  log   [20:18:55.538] [info][canvas][plugins] Setting up plugin
  log   [20:18:55.544] [info][plugins][timelion] Setting up plugin
  log   [20:18:55.545] [info][features][plugins] Setting up plugin
  log   [20:18:55.546] [info][plugins][security] Setting up plugin
  log   [20:18:55.548] [warning][config][plugins][security] Generating a random key for xpack.security.encryptionKey. To prevent sessions from
 being invalidated on restart, please set xpack.security.encryptionKey in kibana.yml
  log   [20:18:55.548] [warning][config][plugins][security] Session cookies will be transmitted over insecure connections. This is not recomme
nded.
  log   [20:18:55.568] [info][apm_oss][plugins] Setting up plugin
  log   [20:18:55.568] [info][plugins][translations] Setting up plugin
  log   [20:18:55.569] [info][data][plugins] Setting up plugin
  log   [20:18:55.574] [info][plugins][share] Setting up plugin
  log   [20:18:55.576] [info][home][plugins] Setting up plugin
  log   [20:18:55.581] [info][plugins][spaces] Setting up plugin
  log   [20:18:55.586] [info][cloud][plugins] Setting up plugin
  log   [20:18:55.587] [info][apm][plugins] Setting up plugin
  log   [20:18:55.639] [info][graph][plugins] Setting up plugin
  log   [20:18:55.643] [info][bfetch][plugins] Setting up plugin
  log   [20:18:55.650] [info][savedobjects-service] Waiting until all Elasticsearch nodes are compatible with Kibana before starting saved obj
ects migrations...
  log   [20:18:56.870] [info][savedobjects-service] Starting saved objects migrations
  log   [20:18:56.930] [info][savedobjects-service] Creating index .kibana_task_manager_1.
```

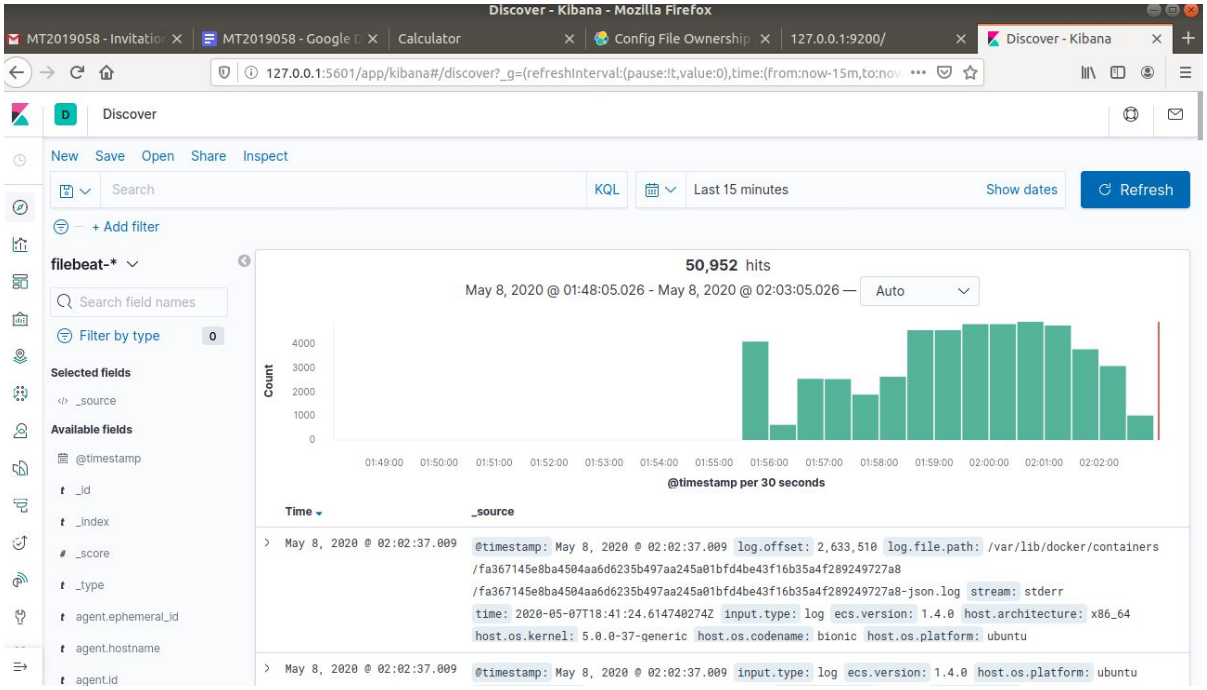
- Start filebeat-
  Run **sudo ./filebeat -e v**


utsav@utsav-HP-Laptop-14q-cs0xxx: ~/Utsav/IIIT-B/SecondSem/SPE/DevOps/filebeat-7.6.2-linux-x86_64
File Edit View Search Terminal Help

```
chown: changing ownership of 'filebeat.yml': Operation not permitted
utsav@utsav-HP-Laptop-14q-cs0xxx:~/Utsav/IIIT-B/SecondSem/SPE/DevOps/filebeat-7.6.2-linux-x86_64$ sudo chown root filebeat.yml
utsav@utsav-HP-Laptop-14q-cs0xxx:~/Utsav/IIIT-B/SecondSem/SPE/DevOps/filebeat-7.6.2-linux-x86_64$ sudo ./filebeat -e -v
2020-05-08T01:54:26.205+0530    INFO    instance/beat.go:622    Home path: [/home/utsav/Utsav/IIIT-B/SecondSem/SPE/DevOps/filebeat-7.6.2-linux
-x86_64] Config path: [/home/utsav/Utsav/IIIT-B/SecondSem/SPE/DevOps/filebeat-7.6.2-linux-x86_64] Data path: [/home/utsav/Utsav/IIIT-B/SecondS
em/SPE/DevOps/filebeat-7.6.2-linux-x86_64/data] Logs path: [/home/utsav/Utsav/IIIT-B/SecondSem/SPE/DevOps/filebeat-7.6.2-linux-x86_64/logs]
2020-05-08T01:54:26.329+0530    INFO    instance/beat.go:630    Beat ID: 6064a2b5-5424-454f-80da-4fb01542ea9a
2020-05-08T01:54:29.526+0530    INFO    add_cloud_metadata/add_cloud_metadata.go:89     add_cloud_metadata: hosting provider type not detected
.
2020-05-08T01:54:31.865+0530    INFO    [seccomp]       seccomp/seccomp.go:124  Syscall filter successfully installed
2020-05-08T01:54:31.886+0530    INFO    [beat]  instance/beat.go:958    Beat info       {"system_info": {"beat": {"path": {"config": "/home/ut
sav/Utsav/IIIT-B/SecondSem/SPE/DevOps/filebeat-7.6.2-linux-x86_64", "data": "/home/utsav/Utsav/IIIT-B/SecondSem/SPE/DevOps/filebeat-7.6.2-linu
x-x86_64/data", "home": "/home/utsav/Utsav/IIIT-B/SecondSem/SPE/DevOps/filebeat-7.6.2-linux-x86_64", "logs": "/home/utsav/Utsav/IIIT-B/SecondS
em/SPE/DevOps/filebeat-7.6.2-linux-x86_64/logs"}, "type": "filebeat", "uuid": "6064a2b5-5424-454f-80da-4fb01542ea9a"}}}
2020-05-08T01:54:31.886+0530    INFO    [beat]  instance/beat.go:967    Build info      {"system_info": {"build": {"commit": "d57bcf8684602e15
000d65b75afcd110e2b12b59", "libbeat": "7.6.2", "time": "2020-03-26T05:23:38.000Z", "version": "7.6.2"}}}
2020-05-08T01:54:31.886+0530    INFO    [beat]  instance/beat.go:970    Go runtime info {"system_info": {"go": {"os":"linux","arch":"amd64","m
ax_procs":4,"version":"go1.13.8"}}}
2020-05-08T01:54:31.899+0530    INFO    [beat]  instance/beat.go:974    Host info       {"system_info": {"host": {"architecture":"x86_64","boo
t_time":"2020-05-08T01:36:57+05:30","containerized":false,"name":"utsav-HP-Laptop-14q-cs0xxx","ip":["127.0.0.1/8","::1/128","192.168.0.103/24"
,"fe80::7978:2b88:a349:f340/64","172.17.0.1/16","fe80::42:3fff:fef9:2af7/64","fe80::44b7:35ff:fe11:96d3/64"],"kernel_version":"5.0.0-37-generi
c","mac":["c8:d9:d2:d2:31:02","74:40:bb:40:61:43","02:42:3f:f9:2a:f7","46:b7:35:11:96:d3"],"os":{"family":"debian","platform":"ubuntu","name":
"Ubuntu","version":"18.04.3 LTS (Bionic Beaver)","major":18,"minor":4,"patch":3,"codename":"bionic"},"timezone":"IST","timezone_offset_sec":19
800,"id":"81be7c3e9dc04a9694557be94d73696b"}}}
2020-05-08T01:54:31.905+0530    INFO    [beat]  instance/beat.go:1003   Process info    {"system_info": {"process": {"capabilities": {"inherit
able":null,"permitted":["chown","dac_override","dac_read_search","fowner","fsetid","kill","setgid","setuid","setpcap","linux_immutable","net_b
ind_service","net_broadcast","net_admin","net_raw","ipc_lock","ipc_owner","sys_module","sys_rawio","sys_chroot","sys_ptrace","sys_pacct","sys_
admin","sys_boot","sys_nice","sys_resource","sys_time","sys_tty_config","mknod","lease","audit_write","audit_control","setfcap","mac_override"
,"mac_admin","syslog","wake_alarm","block_suspend","audit_read"],"effective":["chown","dac_override","dac_read_search","fowner","fsetid","kill
","setgid","setuid","setpcap","linux_immutable","net_bind_service","net_broadcast","net_admin","net_raw","ipc_lock","ipc_owner","sys_module","
sys_rawio","sys_chroot","sys_ptrace","sys_pacct","sys_admin","sys_boot","sys_nice","sys_resource","sys_time","sys_tty_config","mknod","lease",
"audit_write","audit_control","setfcap","mac_override","mac_admin","syslog","wake_alarm","block_suspend","audit_read"],"bounding":["chown","da
c_override","dac_read_search","fowner","fsetid","kill","setgid","setuid","setpcap","linux_immutable","net_bind_service","net_broadcast","net_a
dmin","net_raw","ipc_lock","ipc_owner","sys_module","sys_rawio","sys_chroot","sys_ptrace","sys_pacct","sys_admin","sys_boot","sys_nice","sys_r
esource","sys_time","sys_tty_config","mknod","lease","audit_write","audit_control","setfcap","mac_override","mac_admin","syslog","wake_alarm",
"block_suspend","audit_read"],"ambient":null}, "cwd": "/home/utsav/Utsav/IIIT-B/SecondSem/SPE/DevOps/filebeat-7.6.2-linux-x86_64", "exe": "/ho
me/utsav/Utsav/IIIT-B/SecondSem/SPE/DevOps/filebeat-7.6.2-linux-x86_64/filebeat", "name": "filebeat", "pid": 5062, "ppid": 5061, "seccomp": {"
mode":"filter","no_new_privs":true}, "start_time": "2020-05-08T01:54:25.390+0530"}}}
2020-05-08T01:54:31.905+0530    INFO    instance/beat.go:298    Setup Beat: filebeat; Version: 7.6.2
```

- Check -
  http://127.0.0.1:9200
  http://127.0.0.1:5601
  for elasticsearch and kibana

- Open Kibana and check logs based on timestamp -



50,952 hits

May 8, 2020 @ 01:48:05.026 - May 8, 2020 @ 02:03:05.026 —

```
> May 8, 2020 @ 02:02:37.009   @timestamp: May 8, 2020 @ 02:02:37.009 log.offset: 2,633,510 log.file.path: /var/lib/docker/containers
                               /fa367145e8ba4504aa6d6235b497aa245a01bfd4be43f16b35a4f289249727a8
                               /fa367145e8ba4504aa6d6235b497aa245a01bfd4be43f16b35a4f289249727a8-json.log stream: stderr
                               time: 2020-05-07T18:41:24.614740274Z input.type: log ecs.version: 1.4.0 host.architecture: x86_64
                               host.os.kernel: 5.0.0-37-generic host.os.codename: bionic host.os.platform: ubuntu
> May 8, 2020 @ 02:02:37.009   @timestamp: May 8, 2020 @ 02:02:37.009 input.type: log ecs.version: 1.4.0 host.os.platform: ubuntu
```