Log Analysis Tool Read Me

1. Log Analysis Tool Manual

Author: Yuhan Li

1.1. Function Overview

Before using these functions, you should set $JAVA_HOME and $ELA_HOME(path of this tool), and make sure Java version is 1.8X

All these scripts will run $JAVA_HOME/bin/java -cp $ELA_HOME/target/classes:$ELA_HOME/target/dependency/* elk.elastic.App

1.1.1. /bin/addtmp

1.1.1.1. Introduction

Use addtmp to add templates into template base according to log snippet you provided from elasticsearch.

Template base is located under ./log/, named '$log_typeTemplate.txt' and '$log_typeTemplateScore.txt'

Template base files will be created when first run addtmp.

1.1.1.2. Usage

```
./bin/addtmp -t logtype -h hostname -i index -s start_time -e end_time

logtype: it supports
ocssd/gipcd/alert/crsd/ohasd_orarootagent_root/rootcrs/ohasd_oraagent_crsusr/asm_alert/

hostname: it's name of the host where the logs locate originally.

index: index name the logs stores in elasticsearch
```

1.1.2. /bin/scorelog

1.1.2.1. Introduction

Use scorelog to filter logs with specify scores. You could provide a set of scores and log snippets, it will result log lines which belong to templates with these scores.

Templates and scores maps are store in ./log/$log_typeTemplateScore.txt. Scores are stored at the end of log lines, like 'log_line--4'.

1.1.2.2. Usage

```
./bin/scorelog -t log_type -h hostname -i index -s start_time -e end_time -n setOfScores(splitted by comma)

logtype: it supports
ocssd/gipcd/alert/crsd/ohasd_orarootagent_root/rootcrs/ohasd_oraagent_crsusr/asm_alert/

hostname: it's name of the host where the logs locate originally.

index: index name the logs stores in elasticsearch

setOfScores: e.g. 2,3,4
```

1.1.3. /bin/appearance

1.1.3.1. Introduction

It is used to calulate the numbers of appearance for every template in template base.

Result will be printed on the screen.

1.1.3.2. Usage

```
./bin/appearance -t log_type -h hostname -i index -s start_time -e end_time -n setOfScore

logtype: it supports
ocssd/gipcd/alert/crsd/ohasd_orarootagent_root/rootcrs/ohasd_oraagent_crsusr/asm_alert/

hostname: it's name of the host where the logs locate originally.

index: index name the logs stores in elasticsearch

setOfScores: e.g. 2,3,4
```

1.1.4. /bin/replaceRawAsTmp

1.1.4.1. Introduction

It is used to replace lines of raw logs with templates in template base.

It's a key step for LCS analysis.

1.1.4.2. Usage

```
./bin/replaceRawAsTmp -t log_type -h hostname -i index

logtype: it supports
ocssd/gipcd/alert/crsd/ohasd_orarootagent_root/rootcrs/ohasd_oraagent_crsusr/asm_alert/

hostname: it's name of the host where the logs locate originally.

index: index name the logs stores in elasticsearch
```

1.1.5. /bin/builMatrix

1.1.5.1. Introduction

It is used to build a matrix, which shows the numbers of appearance of templates in multiple log files.

For example:

[1,2

3,4]

This Matrix shows template1 appears once in the first file and twice in the second file. And template2 appears 3 times in the first file and 4 times in the second file.

Result will be printed on screen.

1.1.5.2. Usage

```
./bin/buildMatrix -t log_type -h hostname -i index -p path[]

logtype: it supports
ocssd/gipcd/alert/crsd/ohasd_orarootagent_root/rootcrs/ohasd_oraagent_crsusr/asm_alert/

hostname: it's name of the host where the logs locate originally.

index: index name the logs stores in elasticsearch

path[]: set of paths of log files, separated by comma.
```

1.1.6. /bin/matForEveryFile

1.1.6.1. Introduction

It's used to build matrix for every file. And for a file with N log lines, matrix will be N*N size. Values of the matrix means distances between log lines.

For example:

[0,1

1,0]

It represents a two-line log file, and distance between log line 1 and log line 2 is 1.

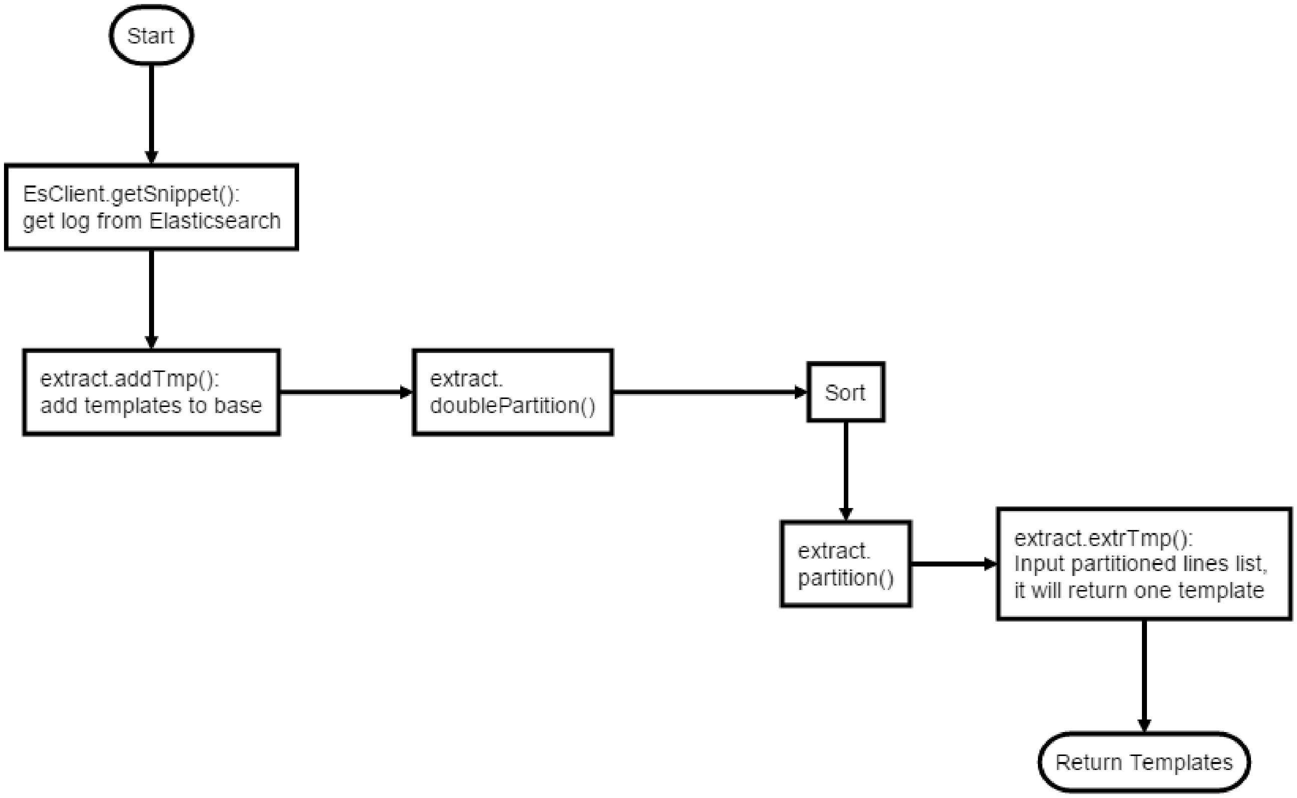
Result will be printed on screen.

1.1.6.2. Usage

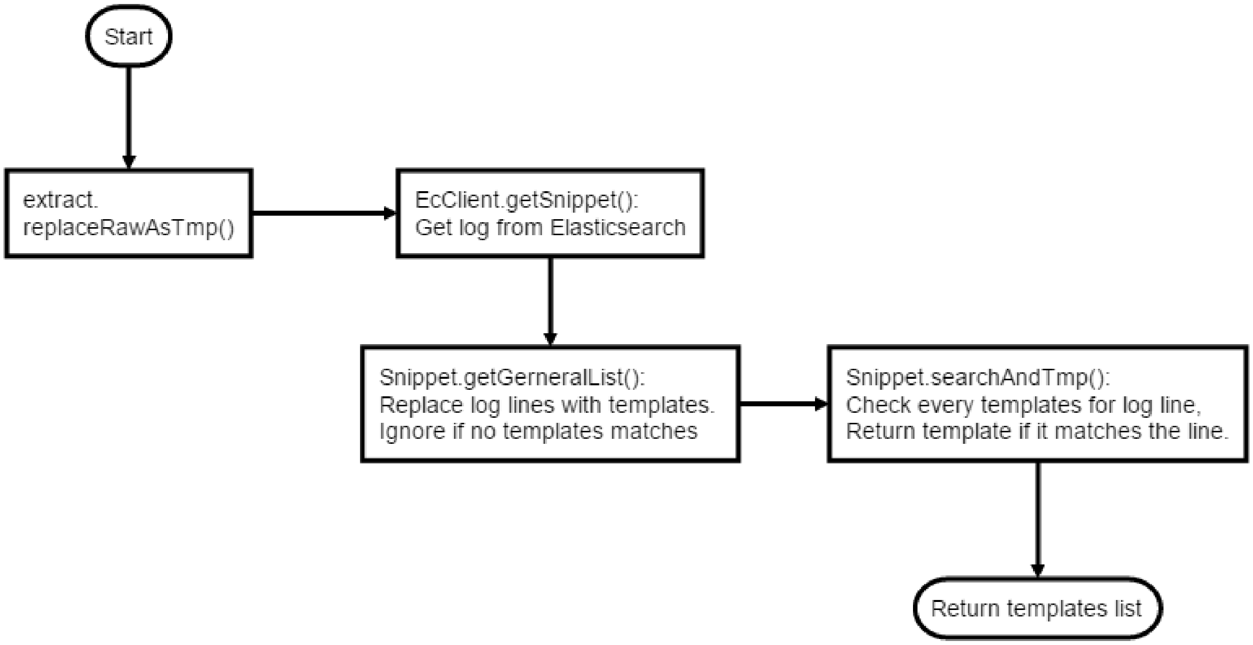
```
./bin/matForEveryFile -t log_type -h hostname -i index

logtype: it supports
ocssd/gipcd/alert/crsd/ohasd_orarootagent_root/rootcrs/ohasd_oraagent_crsusr/asm_alert/

hostname: it's name of the host where the logs locate originally.

index: index name the logs stores in elasticsearch
```

1.2. Function Workflow

1.2.1. /bin/addtmp workflow



1.2.2. /bin/replaceRawAsTmp workflow


Start
extract.
replaceRawAsTmp()
EcClient.getSnippet():
Get log from Elasticsearch
Snippet.getGerneralList():
Replace log lines with templates.
Ignore if no templates matches
Snippet.searchAndTmp():
Check every templates for log line,
Return template if it matches the line.
Return templates list