

# Readme

---

## Step1 环境配置

---

### 1.1 Java环境安装

注意我们的项目是需要Linux系统下运行，所以需要预先安装一个Linux系统

**下载tar.gz的压缩包，这里使用官网下载。**

进入：

<http://www.oracle.com/technetwork/java/javase/downloads/jdk8-downloads-2133151.html>

#### 下载完成后解压到指定文件下

先创建java文件目录，如果已存在就不用创建

```
mkdir -p /usr/local/java
tar -vzxf jdk-8u161-linux-x64.tar.gz -C /usr/local/java/
```

#### 添加环境变量，编辑配置文件

```
vi /etc/profile
在文件最下方或者指定文件添加
export JAVA_HOME=/usr/local/java/jdk1.8.0_161
export CLASSPATH=$CLASSPATH:$JAVA_HOME/lib/
export PATH=$PATH:$JAVA_HOME/bin
```

#### 保存退出

```
source /etc/profile
```

```
java -version
可以看到一下信息则表示配置成功
java version "1.8.0_161"
Java™ SE Runtime Environment (build 1.8.0_161-b12)
Java HotSpot™ 64-Bit Server VM (build 25.161-b12, mixed mode)
```

### 1.2Maven环境配置

---

官网下载 <http://maven.apache.org/download.cgi>

#### 下载并解压

```
cd /usr/local/maven/
tar -zxvf apache-maven-3.8.1-bin.tar.gz
```

## 配置环境变量

```
# 编辑配置文件
vim /etc/profile

# 在末尾追加
export MAVEN_HOME=/usr/local/maven/apache-maven-3.8.1
export PATH=${PATH}:${MAVEN_HOME}/bin

# 使配置文件生效
source /etc/profile
```

## 测试

```
mvn -v

# 返回
Apache Maven 3.8.1 (05c21c65bdfed0f71a2f2ada8b84da59348c4c5d)
Maven home: /usr/local/maven/apache-maven-3.8.1
Java version: 1.8.0_291, vendor: Oracle Corporation, runtime:
/usr/local/java/jdk1.8.0_291/jre
Default locale: en_US, platform encoding: UTF-8
OS name: "linux", version: "3.10.0-1127.18.2.el7.x86_64", arch: "amd64", family:
"unix"
```

## 1.3 Docker环境配置

[可参考官方的配置教程](#)

## 1.4 Redis 环境安装

进入官网找下载 <https://redis.io/download>

```
#选择复制链接
wget http://download.redis.io/releases/redis-5.0.7.tar.gz

#解压

tar -zxvf redis-5.0.7.tar.gz

# 将redis目录放置到 /usr/local/redis目录
mv /root/redis-5.0.7 /usr/local/redis

#编译
cd /usr/local/redis
make

#安装
make PREFIX=/usr/local/redis install

#启动redis
```

```
./bin/redis-server& ./redis.conf
```

## Step2 运行项目

```
git clone https://github.com/HuskiesUESTC/AntFuzzer-WASMOD.git
```

首先在项目中新建config文件夹，并创建test.json的配置文件

```
{
  "fuzzers": [
    {
      "vulnerability": "BlockDependency-MissingAuth",
      "arg_driver": "afl",
      "iteration": 100
    },
    {
      "vulnerability": "FakeEOSTransfer",
      "arg_driver": "afl",
      "iteration": 100
    },
    {
      "vulnerability": "ForgedNotification",
      "arg_driver": "afl",
      "iteration": 100
    },
    {
      "vulnerability": "HackRecipient",
      "arg_driver": "afl",
      "iteration": 100
    },
    {
      "vulnerability": "MissingAuth",
      "arg_driver": "afl",
      "iteration": 100
    },
    {
      "vulnerability": "Rollback",
      "arg_driver": "afl",
      "iteration": 100
    }
  ],
  "output_file": "./result/TestAllAFL.json",
  "smart_contract_dir": "/root/EOSFuzzer/dataset/contracts"
}
```

其中smart\_contract\_dir是自己合约的文件地址（docker里面的地址）。

ravatarcafe	keepscore	members	mutualcredit	owdinn
ello	kingofeos	merkle	mydao	pandaf
ello.target	lottery1	monstereosio	myprofile	pet
nfiniverse	lover	more.moment	newapp1	pex
ntoverflow	masteroracle	more.voting	oracle.new	pradat

然后将项目整体挂到Docker上

```
docker run -d -it --name AntFuzzer -v /home/coldplay/Desktop/AntFuzzer/AntFuzzer-WASMOD-main:/root/AntFuzzer ubuntu /bin/bash
```

其中AntFuzzer是项目名称：前面是项目所在位置 后面是docker下所在位置 最后的是使用的镜像

```
docker exec -it AntFuzzer bash
```

执行上述的命令进入容器中。

```
root@ubuntu:/home/coldplay/Desktop# cd AntFuzzer/AntFuzzer-WASMOD-main/
root@ubuntu:/home/coldplay/Desktop/AntFuzzer/AntFuzzer-WASMOD-main# ls -lh
总用量 44K
drwxrwxr-x 2 coldplay coldplay 4.0K 11月 2 03:20 config
-rw-rw-r-- 1 coldplay coldplay 164 4月 5 2022 debug.sh
drwxrwxr-x 4 coldplay coldplay 4.0K 4月 5 2022 fuzz
drwxrwxr-x 2 coldplay coldplay 4.0K 4月 5 2022 log
-rw-rw-r-- 1 coldplay coldplay 3.5K 11月 1 10:38 main.py
-rwxrwxrwx 1 coldplay coldplay 138 4月 5 2022 mvn.sh
-rw-rw-r-- 1 coldplay coldplay 2.0K 4月 5 2022 pom.xml
drwxrwxr-x 2 coldplay coldplay 4.0K 4月 5 2022 script
drwxrwxr-x 3 coldplay coldplay 4.0K 4月 5 2022 src
-rwxrwxrwx 1 coldplay coldplay 154 4月 5 2022 start.sh
drwxr-xr-x 5 root root 4.0K 11月 1 10:38 target
```

然后将Redis启动

```
root@57129d66587e:/usr/bin# ./redis-server
671:C 02 Nov 14:36:10.382 # 0000000000000000 Redis is starting 0000000000000000
671:C 02 Nov 14:36:10.382 # Redis version=4.0.9, bits=64, commit=00000000, modified=0, pid=671, just started
671:C 02 Nov 14:36:10.382 # Warning: no config file specified, using the default config. In order to specify a config file use ./redis-server /path/to/redis.conf

Redis 4.0.9 (00000000/0) 64 bit

Running in standalone mode
Port: 6379
PID: 671

http://redis.io

671:M 02 Nov 14:36:10.387 # Server initialized
671:M 02 Nov 14:36:10.387 # WARNING overcommit memory is set to 0! Background save may fail under low memory condition. To fix this issue add 'vm.overcommit_memory = 1' to /etc/sysctl.conf and then reboot or run the command 'sysctl vm.overcommit_memory=1' for this to take effect.
671:M 02 Nov 14:36:10.387 # WARNING you have Transparent Huge Pages (THP) support enabled in your kernel. This will create latency and memory usage issues with Redis. To fix this issue run the command 'echo never > /sys/kernel/mm/transparent_hugepage/enabled' as root, and add it to your /etc/rc.local in order to retain the setting after a reboot. Redis must be restarted after THP is disabled.
671:M 02 Nov 14:36:10.387 * Ready to accept connections
```

运行./start.sh命令启动项目

```

root@57129d66587e:~/AntFuzzer# ./start.sh
[INFO] Scanning for projects...
[INFO]
[INFO] -----< edu.uestc:AntFuzzer >-----
[INFO] Building AntFuzzer 1.0-SNAPSHOT
[INFO] -----[ jar ]-----
[INFO]
[INFO] --- maven-clean-plugin:2.5:clean (default-clean) @ AntFuzzer ---
[INFO] Deleting /root/.AntFuzzer/target
[INFO]
[INFO] BUILD SUCCESS
[INFO]
[INFO] Total time: 0.472 s
[INFO] Finished at: 2023-11-02T14:38:09Z
[INFO]
[INFO] Scanning for projects...
[INFO]
[INFO] -----< edu.uestc:AntFuzzer >-----
[INFO] Building AntFuzzer 1.0-SNAPSHOT
[INFO] -----[ jar ]-----
[INFO]
[INFO] --- maven-resources-plugin:2.6:resources (default-resources) @ AntFuzzer ---
[INFO] Using 'UTF-8' encoding to copy filtered resources.
[INFO] Copying 47 resources
[INFO]
[INFO] --- maven-compiler-plugin:3.1:compile (default-compile) @ AntFuzzer ---
[INFO] Changes detected - recompiling the module!
[INFO] Compiling 115 source files to /root/.AntFuzzer/target/classes
[WARNING] /root/.AntFuzzer/src/main/java/edu/uestc/antfuzzer/framework/core/BeanFactory.java: Some input files use unchecked or unsafe operations.
[WARNING] /root/.AntFuzzer/src/main/java/edu/uestc/antfuzzer/framework/core/BeanFactory.java: Recompile with -Xlint:unchecked for details.
[INFO]
[INFO] BUILD SUCCESS

```

项目会首先通过maven进行jar包的打包build过程等等，然后开始通过红箭头标记的命令进入主函数，并且传递配置文件的参数

```

1  ►  #!/usr/bin/env bash
2      mvn clean
3      mvn compile
4  ➡  mvn -e exec:java -Dexec.mainClass="edu.uestc.antfuzzer.Main" -Dexec.args="-fuzzingConfigFile ./config/test.json"

```

运行过程如下：

```

cleos create account eosio eosio.token EOS6MRyAjQq8ud7hVNYcfnVPJqcVpscN5So8BhtHuGYqET5GDW5CV
# eosio <= eosio::newaccount {"creator":"eosio","name":"eosio.token","owner":{"threshold":1,"keys":[{"key":"EOS6MRyAjQq8ud7hVNYcfnVPJqcVpscN5So8BhtHuGYqET5GDW5CV"}]}}
...
executed transaction: c847868a7dc45e131d74f5d9d63941a8472e2de9bc719c7fcd9c2ea128f8db6 200 bytes 290 uswarn 2023-11-02T14:38:24.426 thread-0 mai
n.cpp:487 print_result warning: transaction executed locally, but may not be confirmed by the network yet
cleos set contract eosio.token /root/.AntFuzzer/target/classes
cleos push action eosio.token create ["eosio","10000000000000000000 EOS"] -p eosio.token@active -f 2>&1
executed transaction: 87b9cca322d20be1c43ec14fda8c4209c318597c6e8839c78f0ac40d5972e621 144 bytes 2652 uswarn 2023-11-02T14:38:24.527 thread-0 mai
n.cpp:487 print_result warning: transaction executed locally, but may not be confirmed by the network yet# eosio.null
<= eosio.null::nonce "52b915572c090600"# eosio.token <= eosio.token::create {"issuer":"eosio","maximum_supply":"10000000000000000000 EOS"}
cleos create account eosio testeosfrom EOS6MRyAjQq8ud7hVNYcfnVPJqcVpscN5So8BhtHuGYqET5GDW5CV
# eosio <= eosio::newaccount {"creator":"eosio","name":"testeosfrom","owner":{"threshold":1,"keys":[{"key":"EOS6MRyAjQq8ud7hVNYcfnVPJqcVpscN5So8BhtHuGYqET5GDW5CV"}]}}
...
executed transaction: c5c53de1e49b5fb5f68178b24917c8d6138636b8780b08e93dc7a2d42e923fe8 200 bytes 249 uswarn 2023-11-02T14:38:24.555 thread-0 mai
n.cpp:487 print_result warning: transaction executed locally, but may not be confirmed by the network yet
cleos push action eosio.token issue ["testeosfrom","10000000000000000000 EOS","FUZZER"] -p eosio@active -f 2>&1
executed transaction: ff2dee7538b124b6f6137838536cfed85f55c7353a20105ac6b69c2402d4c29e 152 bytes 5474 uswarn 2023-11-02T14:38:24.591 thread-0 mai
n.cpp:487 print_result warning: transaction executed locally, but may not be confirmed by the network yet# eosio.null
<= eosio.null::nonce "11b616572c090600"# eosio.token <= eosio.token::issue {"to":"testeosfrom","quantity":"1000000000.0000 EOS","memo":"FUZZER"}#
eosio.token <= eosio.token::transfer {"from":"eosio","to":"testeosfrom","quantity":"1000000000.0000 EOS","memo":"FUZZER"}#
eosio.token <= eosio.token::transfer {"from":"eosio","to":"testeosfrom","quantity":"1000000000.0000 EOS","memo":"FUZZER"}#
eosio.token <= eosio.token::transfer {"from":"eosio","to":"testeosfrom","quantity":"1000000000.0000 EOS","memo":"FUZZER"}#
cleos create account eosio tungsten EOS6MRyAjQq8ud7hVNYcfnVPJqcVpscN5So8BhtHuGYqET5GDW5CV
# eosio <= eosio::newaccount {"creator":"eosio","name":"tungsten","owner":{"threshold":1,"keys":[{"key":"EOS6MRyAjQq8ud7hVNYcfnVPJqcVpscN5So8BhtHuGYqET5GDW5CV"}]}}
...
executed transaction: c889930debfc96a8e66de2ae15391403326629c229e7b32ea8cfa79dda32e11d 200 bytes 512 uswarn 2023-11-02T14:38:24.621 thread-0 mai
n.cpp:487 print_result warning: transaction executed locally, but may not be confirmed by the network yet
cleos push action eosio.token issue ["tungsten","1000000000.0000 EOS","FUZZER"] -p eosio@active -f 2>&1
executed transaction: 4d2de46236e8820b252ab3ea0c5971a39b586f0bae304afa1b65dccc9975858595 152 bytes 10486 uswarn 2023-11-02T14:38:24.658 thread-0 mai
n.cpp:487 print_result warning: transaction executed locally, but may not be confirmed by the network yet# eosio.null
<= eosio.null::nonce "9aa117572c090600"# eosio.token <= eosio.token::issue {"to":"tungsten","quantity":"1000000000.0000 EOS","memo":"FUZZER"}#
eosio.token <= eosio.token::transfer {"from":"eosio","to":"tungsten","quantity":"1000000000.0000 EOS","memo":"FUZZER"}#
eosio.token <= eosio.token::transfer {"from":"eosio","to":"tungsten","quantity":"1000000000.0000 EOS","memo":"FUZZER"}#
eosio.token <= eosio.token::transfer {"from":"eosio","to":"tungsten","quantity":"1000000000.0000 EOS","memo":"FUZZER"}#

```

最终会得到结果如图所示

包括name,starttime,time,count,invalidArgumentCount,coverage等等结果

