

Prerequisites

Make sure you have the following:

- WSL2 with Ubuntu 22.04 or
- Git
- Python 3.10
- Java 11 or 17 (for Flink
- Kafka and Zookeeper (manual setup)
- Redis, ClickHouse (manual setup)
- Kong Gateway (running outside WSL or on local Linux
- curl, wget, net-tools, unzip, jq

1 System Update and Basic Packages

- ☐ sudo apt update && sudo apt upgrade -y
- ☐ sudo apt install -y git python3 python3-pip python3-venv openjdk-17-jdk curl net-tools redis-server unzip jq

2 Clone Both Repositories

- ☐ git clone <https://github.com/S-idd/AADS-APIABUSEDECETECTIONSISTEM--PythonFile.git>
- ☐ git clone <https://github.com/S-idd/APIABUSEDECETECTIONSISTEM.git>

3 Set Up Python Environment

- ☐ cd AADS-APIABUSEDECETECTIONSISTEM--PythonFile
- ☐ python3 -m venv venv
- ☐ source venv/bin/activate

Manually Install Required Python Packages

- ☐ pip install kafka-python requests redis

4 Install and Start Kafka & Zookeeper

Install Kafka

- ☐ cd ~wget https://downloads.apache.org/kafka/3.7.0/kafka_2.13-3.7.0.tgz
- ☐ tar -xvzf kafka_2.13-3.7.0.tgz
- ☐ mv kafka_2.13-3.7.0 kafka

● Start Zookeeper

- ☐ `cd ~/kafka`
- ☐ `bin/zookeeper-server-start.sh config/zookeeper.properties`

Open a new terminal before continuing.

● Start Kafka

- ☐ `cd ~/kafka`
- ☐ `bin/kafka-server-start.sh config/server.properties`

5 Create Kafka Topic

- ☐ `cd ~/kafka`
- ☐ `bin/kafka-topics.sh --create --topic kong-logs --bootstrap-server localhost:9092 --replication-factor 1 --partitions 1`

6 Set Up Kong Gateway (Outside WSL or Linux in WSL)

Make sure Kong Admin API is accessible via `localhost:8001`.

Example Route & Plugin Setup

- ☐ `curl -i -X POST http://localhost:8001/services/ \`
`--data name=example \`
`--data url='http://httpbin.org'`
- ☐ `curl -i -X POST http://localhost:8001/services/example/routes \`
`--data 'paths[]=api'`
- ☐ `curl -i -X POST http://localhost:8001/plugins \`
`--data "name=file-log" \`
`--data "config.path=/tmp/kong-logs.txt"`

7 Start the Python Log Analyzer

- ☐ `cd ~/AADS-APIABUSEDETECTIONSYSTEM--PythonFile`
- ☐ `source venv/bin/activate`
- ☐ `python responder.py`

8] Simulate API Abuse for Testing

☐ for i in {1..50}; do curl http://localhost:8000/api/get; done

✓ Useful Commands

☐ # Start Zookeeper
~/kafka/bin/zookeeper-server-start.sh ~/kafka/config/zookeeper.properties

☐ # Start Kafka
~/kafka/bin/kafka-server-start.sh ~/kafka/config/server.properties

☐ # Start Redis
sudo service redis-server start

☐ # Tail Kong logs (if using file-log)
tail -f /tmp/kong-logs.txt

Command's

- ```

Zookeeper X + v
hannadisiiddarth@siiddarth: ~ % cd kafka
hannadisiiddarth@siiddarth: ~ % ./bin/zookeeper-server-start.sh config/zookeeper.properties
2025-07-27 10:34:23,390 INFO Reading configuration from: config/zookeeper.properties (org.apache.zookeeper.server.quorum.QuorumPeerConfig)
2025-07-27 10:34:23,390 WARN config/zookeeper.properties is relative. Prepend ./ to indicate that you're sure! (org.apache.zookeeper.server.quorum.QuorumPeerConfig)
2025-07-27 10:34:23,392 INFO clientPortAddress is 0.0.0.0:2181 (org.apache.zookeeper.server.quorum.QuorumPeerConfig)
2025-07-27 10:34:23,392 INFO secureClientPort is not set (org.apache.zookeeper.server.quorum.QuorumPeerConfig)
2025-07-27 10:34:23,392 INFO observerMasterPort is not set (org.apache.zookeeper.server.quorum.QuorumPeerConfig)
2025-07-27 10:34:23,393 INFO metricsProvider.className is org.apache.zookeeper.metrics.impl.DefaultMetricsProvider (org.apache.zookeeper.server.quorum.QuorumPeerConfig)
2025-07-27 10:34:23,393 INFO autopurge.snapshotInterval set to 3 (org.apache.zookeeper.server.DataDirCleanupManager)
2025-07-27 10:34:23,395 INFO autopurge.purgeInterval set to 0 (org.apache.zookeeper.server.DataDirCleanupManager)
2025-07-27 10:34:23,395 INFO Purge task is not scheduled. (org.apache.zookeeper.server.DataDirCleanupManager)
2025-07-27 10:34:23,395 WARN Either no config or no quorum defined in config, running in standalone mode (org.apache.zookeeper.server.quorum.QuorumPeerMain)
2025-07-27 10:34:23,396 INFO Log4j 1.2 jmx support not found; jmx disabled. (org.apache.zookeeper.jmx.ManagedUtil)
2025-07-27 10:34:23,397 INFO Reading configuration from: config/zookeeper.properties (org.apache.zookeeper.server.quorum.QuorumPeerConfig)
2025-07-27 10:34:23,397 WARN config/zookeeper.properties is relative. Prepend ./ to indicate that you're sure! (org.apache.zookeeper.server.quorum.QuorumPeerConfig)
2025-07-27 10:34:23,397 INFO clientPortAddress is 0.0.0.0:2181 (org.apache.zookeeper.server.quorum.QuorumPeerConfig)
2025-07-27 10:34:23,398 INFO secureClientPort is not set (org.apache.zookeeper.server.quorum.QuorumPeerConfig)
2025-07-27 10:34:23,398 INFO observerMasterPort is not set (org.apache.zookeeper.server.quorum.QuorumPeerConfig)
2025-07-27 10:34:23,398 INFO metricsProvider.className is org.apache.zookeeper.metrics.impl.DefaultMetricsProvider (org.apache.zookeeper.server.quorum.QuorumPeerConfig)
2025-07-27 10:34:23,399 INFO Starting server (org.apache.zookeeper.server.ZooKeeperServerMain)
2025-07-27 10:34:23,412 INFO ServerMetrics initialized with provider org.apache.zookeeper.metrics.impl.DefaultMetricsProvider@4387b79e (org.apache.zookeeper.server.ServerMetrics)
2025-07-27 10:34:23,417 INFO ACL digest algorithm is: SHA1 (org.apache.zookeeper.server.auth.DigestAuthenticationProvider)
2025-07-27 10:34:23,417 INFO Zookeeper.DigestAuthenticationProvider.enabled = true (org.apache.zookeeper.server.auth.DigestAuthenticationProvider)
2025-07-27 10:34:23,426 INFO zookeeper.snapshot.trust.empty = false (org.apache.zookeeper.server.persistence.FileTxnSnapLog)
2025-07-27 10:34:23,429 INFO (org.apache.zookeeper.server.ZooKeeperServer)
2025-07-27 10:34:23,429 INFO (org.apache.zookeeper.server.ZooKeeperServer)
2025-07-27 10:34:23,429 INFO (org.apache.zookeeper.server.ZooKeeperServer)
2025-07-27 10:34:23,430 INFO (org.apache.zookeeper.server.ZooKeeperServer)
2025-07-27 10:34:23,430 INFO (org.apache.zookeeper.server.ZooKeeperServer)
2025-07-27 10:34:23,430 INFO (org.apache.zookeeper.server.ZooKeeperServer)
2025-07-27 10:34:23,430 INFO (org.apache.zookeeper.server.ZooKeeperServer)
2025-07-27 10:34:23,430 INFO (org.apache.zookeeper.server.ZooKeeperServer)
2025-07-27 10:34:23,430 INFO (org.apache.zookeeper.server.ZooKeeperServer)
2025-07-27 10:34:23,433 INFO Server environment:zookeeper.version=3.8.4-9316c2a7a91666db4f593f3d6dfc36cc436c, built on 2024-02-12 22:16 UTC (org.apache.zookeeper.server.ZooKeeperServer)
2025-07-27 10:34:23,433 INFO Server environment:host.name=siiddarth.localdomain (org.apache.zookeeper.server.ZooKeeperServer)
2025-07-27 10:34:23,433 INFO Server environment:java.version=11.0.27 (org.apache.zookeeper.server.ZooKeeperServer)
2025-07-27 10:34:23,433 INFO Server environment:java.vendor=ubuntu (org.apache.zookeeper.server.ZooKeeperServer)
2025-07-27 10:34:23,433 INFO Server environment:java.home=/usr/lib/jvm/java-11-openjdk-amd64 (org.apache.zookeeper.server.ZooKeeperServer)
2025-07-27 10:34:23,433 INFO Server environment:java.class.path=/home/kannadisiiddarth/kafka/bin/./libs/activation-1.1.1.jar:/home/kannadisiiddarth/kafka/bin/./libs/asmalliance-repackaged-2.6.1.jar:/home/kannadisiiddarth/kafka/bin/

```

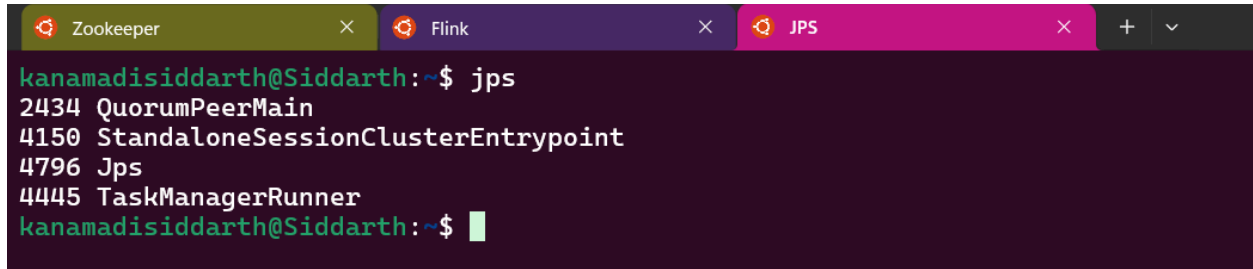
## Command's

- ```
kanamadisiddarth@Siddarth:~$ cd flink-1.17.2/
kanamadisiddarth@Siddarth:~/flink-1.17.2$ ./bin/start-cluster.sh
Starting cluster.
Starting standalone session daemon on host Siddarth.
Starting task executor daemon on host Siddarth.
kanamadisiddarth@Siddarth:~/flink-1.17.2$
```

Step 03 : Check Jobs Are Created Or Not

Command's

☐ jps

A terminal window with tabs for Zookeeper, Flink, and JPS. The JPS tab is active, showing the output of the 'jps' command. The output lists four processes: QuorumPeerMain (PID 2434), StandaloneSessionClusterEntrypoint (PID 4150), Jps (PID 4796), and TaskManagerRunner (PID 4445).

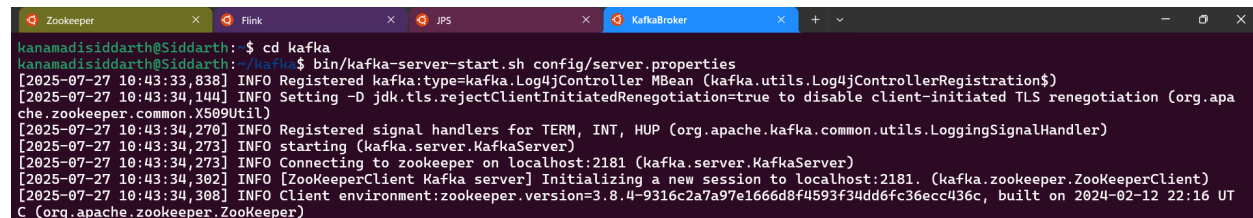
```
kanamadisiddarth@Siddarth:~$ jps
2434 QuorumPeerMain
4150 StandaloneSessionClusterEntrypoint
4796 Jps
4445 TaskManagerRunner
kanamadisiddarth@Siddarth:~$
```

Step 04 :Start Kafka Broker

Command's

☐ cd kafka

☐ bin/kafka-server-start.sh config/server.properties

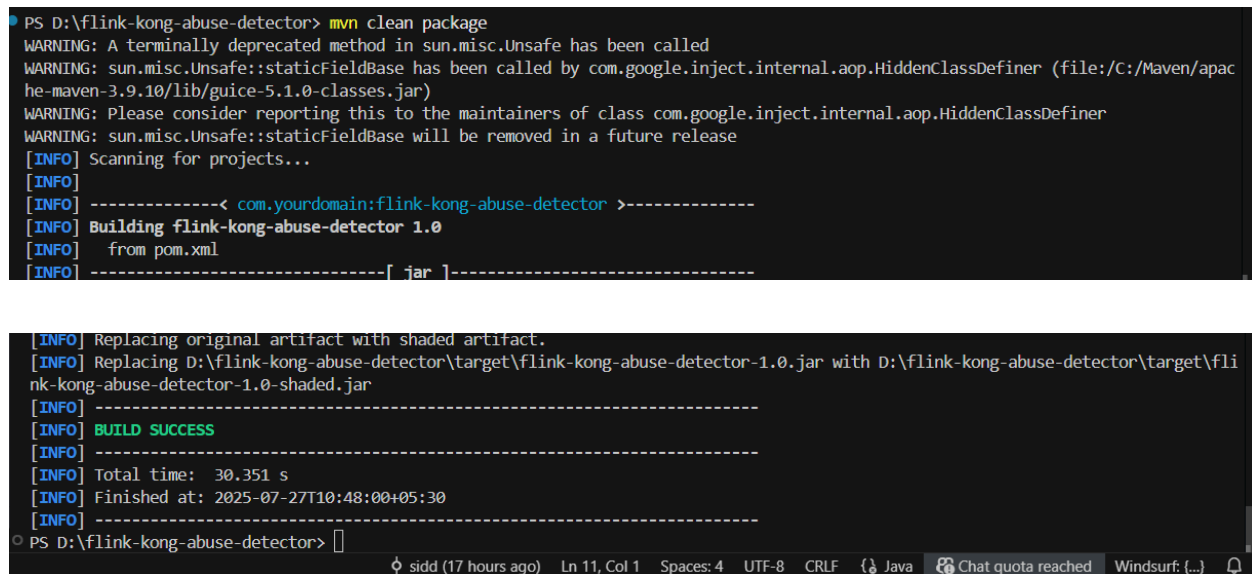
A terminal window with tabs for Zookeeper, Flink, JPS, and KafkaBroker. The KafkaBroker tab is active, showing the output of the 'bin/kafka-server-start.sh config/server.properties' command. The logs show the Kafka server starting, registering with Zookeeper, and connecting to the local Zookeeper instance.

```
kanamadisiddarth@Siddarth:~$ cd kafka
kanamadisiddarth@Siddarth:~/kafka$ bin/kafka-server-start.sh config/server.properties
[2025-07-27 10:43:33,838] INFO Registered kafka:type=kafka.Log4jController MBean (kafka.utils.Log4jControllerRegistration$)
[2025-07-27 10:43:34,144] INFO Setting -Djdk.tls.rejectClientInitiatedRenegotiation=true to disable client-initiated TLS renegotiation (org.apache.zookeeper.common.X509Util)
[2025-07-27 10:43:34,270] INFO Registered signal handlers for TERM, INT, HUP (org.apache.kafka.common.utils.LoggingSignalHandler)
[2025-07-27 10:43:34,273] INFO starting (kafka.server.KafkaServer)
[2025-07-27 10:43:34,273] INFO Connecting to zookeeper on localhost:2181 (kafka.server.KafkaServer)
[2025-07-27 10:43:34,302] INFO [ZooKeeperClient Kafka server] Initializing a new session to localhost:2181. (kafka.zookeeper.ZooKeeperClient)
[2025-07-27 10:43:34,308] INFO Client environment:zookeeper.version=3.8.4-9316c2a7a97e1666d8f4593f34dd6fc36ecc436c, built on 2024-02-12 22:16 UT
C (org.apache.zookeeper.ZooKeeper)
```

Step 05 :Build Your Maven Project

Command

☐ mvn clean package

A terminal window showing the output of the 'mvn clean package' command. The output includes warnings about deprecated methods, scanning for projects, and the successful building of the 'flink-kong-abuse-detector-1.0.jar' file. The build is successful and the artifact is replaced with a shaded version.

```
PS D:\flink-kong-abuse-detector> mvn clean package
WARNING: A terminally deprecated method in sun.misc.Unsafe has been called
WARNING: sun.misc.Unsafe::staticFieldBase has been called by com.google.inject.internal.aop.HiddenClassDefiner (file:/C:/Maven/apache-maven-3.9.10/lib/guice-5.1.0-classes.jar)
WARNING: Please consider reporting this to the maintainers of class com.google.inject.internal.aop.HiddenClassDefiner
WARNING: sun.misc.Unsafe::staticFieldBase will be removed in a future release
[INFO] Scanning for projects...
[INFO]
[INFO] -----< com.yourdomain:flink-kong-abuse-detector >-----
[INFO] Building flink-kong-abuse-detector 1.0
[INFO] from pom.xml
[INFO] -----[ jar ]-----
[INFO] Replacing original artifact with shaded artifact.
[INFO] Replacing D:\flink-kong-abuse-detector\target\flink-kong-abuse-detector-1.0.jar with D:\flink-kong-abuse-detector\target\flink-kong-abuse-detector-1.0-shaded.jar
[INFO]
[INFO] BUILD SUCCESS
[INFO]
[INFO] Total time: 30.351 s
[INFO] Finished at: 2025-07-27T10:48:00+05:30
[INFO]
PS D:\flink-kong-abuse-detector>
```

Step 05: Once After Successful Build

This command It Use Copy The .jar File Generated By mvn clean package Command
Command

- ☐ `cp /mnt/d/flink-kong-abuse-detector/target/flink-kong-abuse-detector-1.0.jar ~/flink-1.17.2/`

```
Zookeeper x Flink x JPS x KafkaBroker x FlinkSubmit x + v
kanamadisiddarth@Siddarth: $ cp /mnt/d/flink-kong-abuse-detector/target/flink-kong-abuse-detector-1.0.jar ~/flink-1.17.2/
kanamadisiddarth@Siddarth: $
```

Step 06: Submit The Job To Flink

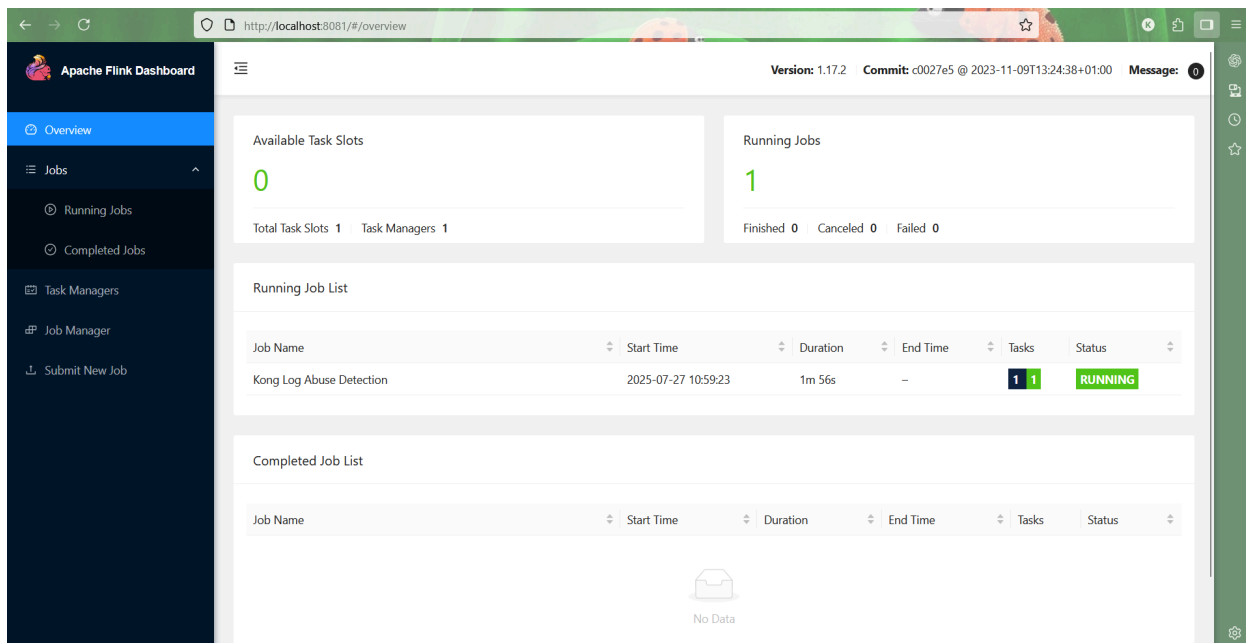
Command's

- ☐ `cd flink-1.17.2/`
- ☐ `./bin/flink run -m localhost:8081 flink-kong-abuse-detector-1.0.jar`

```
Zookeeper x Flink x JPS x KafkaBroker x FlinkSubmit x + v
kanamadisiddarth@Siddarth: $ cp /mnt/d/flink-kong-abuse-detector/target/flink-kong-abuse-detector-1.0.jar ~/flink-1.17.2/
kanamadisiddarth@Siddarth: $ cd flink-1.17.2/
kanamadisiddarth@Siddarth:~/flink-1.17.2$ ./bin/flink run -m localhost:8081 flink-kong-abuse-detector-1.0.jar
>>> Flink KongLogProcessor started.
WARNING: An illegal reflective access operation has occurred
WARNING: Illegal reflective access by org.apache.flink.api.java.ClosureCleaner (file:/home/kanamadisiddarth/flink-1.17.2/lib/flink-dist-1.17.2.jar) to field java.lang.String.value
WARNING: Please consider reporting this to the maintainers of org.apache.flink.api.java.ClosureCleaner
WARNING: Use --illegal-access=warn to enable warnings of further illegal reflective access operations
WARNING: All illegal access operations will be denied in a future release
>>> Connected to Kafka topic: kong-logs
Job has been submitted with JobID 08cd430f7d7546693bf804c903394b5a
```

Step 07: Open Apache Flink Web DashBoard

- ☐ <http://localhost:8081>



Step 08: Check Job In TaskManager Page

Apache Flink Dashboard

Version: 1.17.2 Commit: c0027e5 @ 2023-11-09T13:24:38+01:00 Message: 0

Task Managers

Path, ID	Data Port	Last Heartbeat	All Slots	Free Slots	CPU Cores	Physical MEM	Flink Managed MEM
localhost:37483-d25d1d akka.tcp://flink@localhost:37483/user/rpc/taskmanager_0	38357	2025-07-27 11:03:57	1	0	12	3.50 GB	512 MB

Step 09 :Start Kong

Command

☐ `sudo kong start`

```
kanamadisiddarth@Siddarth:~$ sudo kong start
[sudo] password for kanamadisiddarth:
2025/07/27 11:08:40 [warn] ulimit is currently set to "1024". For better performance set it to at least "4096" using "ulimit -n"
2025/07/27 11:08:40 [warn] ulimit is currently set to "1024". For better performance set it to at least "4096" using "ulimit -n"
2025/07/27 11:08:40 [warn] Found dangling unix sockets in the prefix directory ("/usr/local/kong") while preparing to start Kong. This may be a sign that Kong was previously shut down uncleanly or is in an unknown state and could require further investigation.
2025/07/27 11:08:40 [warn] Attempting to remove dangling sockets before starting Kong...
2025/07/27 11:08:40 [warn] removing unix socket: /usr/local/kong/worker_events.sock
Kong started
```

Step 10 :Run The Python File

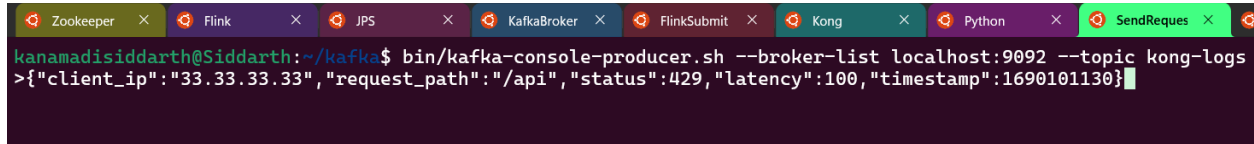
Command

☐ `python3 responder.py`

```
kanamadisiddarth@Siddarth:~$ ls
AAS                                kong_3.6.1_amd64.deb              snap
apache-cassandra-4.1.3-bin.tar.gz flink-1.17.2-bin-scala_2.12.tgz  start-abuse-detection.sh
auth                               fluent                             td-agent-bit_1.9.10_amd64.deb
cassandra                         fluent-bit.conf                   test.js
clickhouse                        interview                          responder.py
config.yaml                       kafka                             path-to-backend
flb_kong_log.db                  kafka_2.13-3.9.1.tgz             ping
kanamadisiddarth@Siddarth:~$ python3 responder.py
Starting abuse responder with loaded YAML config...
```

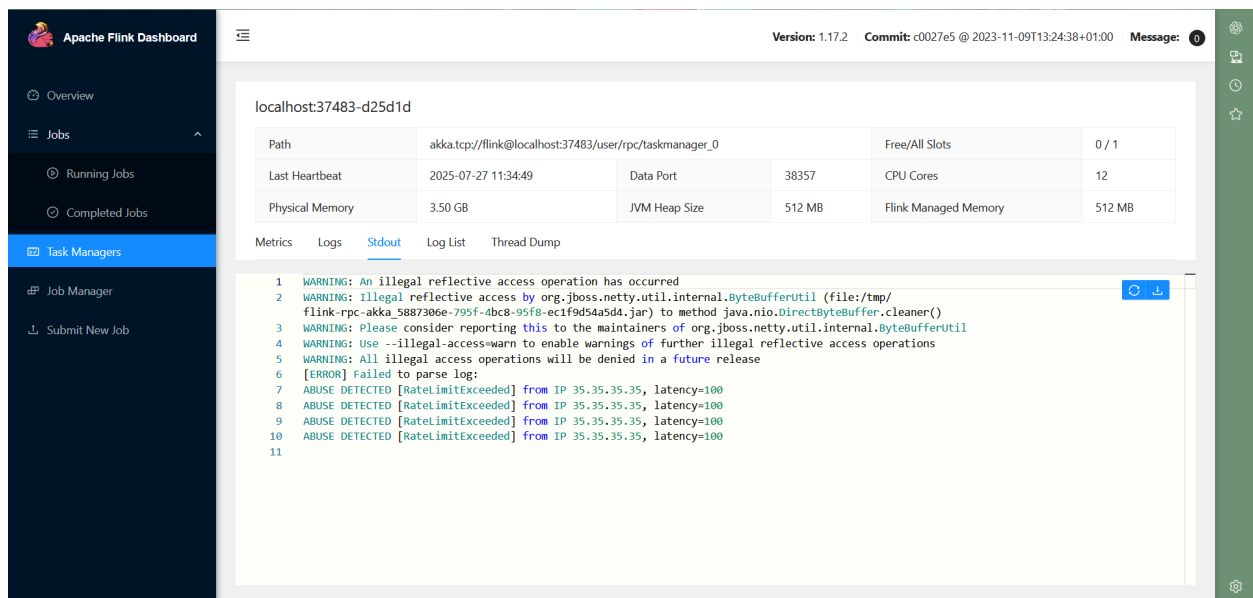

Step 11: Send Request Using Kong And Kafka commands

❑ bin/kafka-console-producer.sh --broker-list localhost:9092 --topic kong-log



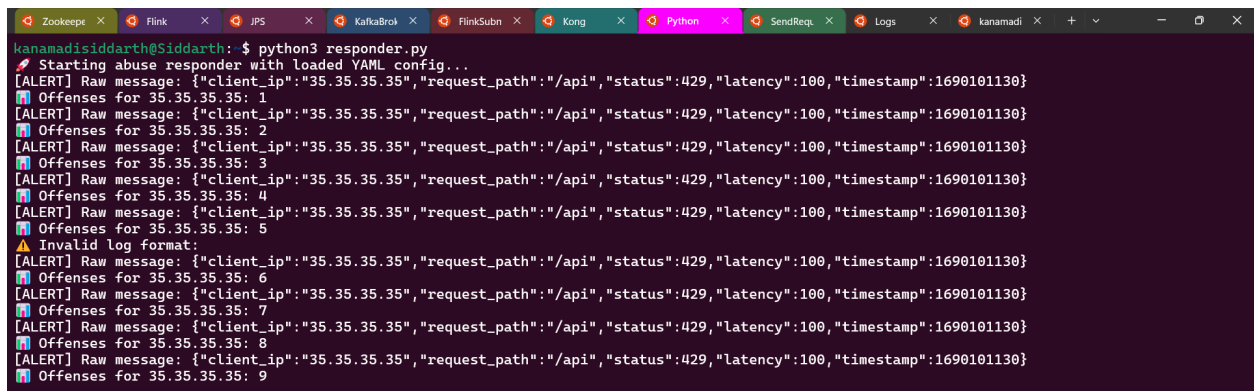
```
kanamadisiddarth@Siddarth:~/kafka$ bin/kafka-console-producer.sh --broker-list localhost:9092 --topic kong-logs
>{"client_ip":"33.33.33.33","request_path":"/api","status":429,"latency":100,"timestamp":1690101130}
```

Step 12: Check In The Web DashBoard



The screenshot shows the Apache Flink Dashboard interface. On the left is a sidebar with navigation options: Overview, Jobs, Task Managers, and Job Manager. The main panel displays details for a task manager with ID 'localhost:37483-d25d1d'. It includes a table with metrics like Path, Last Heartbeat, Physical Memory, Free/All Slots, Data Port, CPU Cores, JVM Heap Size, and Flink Managed Memory. Below the table, there are tabs for Metrics, Logs, Stdout, Log List, and Thread Dump. The 'Stdout' tab is active, showing a log of warnings and errors, including 'WARNING: An illegal reflective access operation has occurred' and 'ABUSE DETECTED [RateLimitExceeded]'.

Step 13: [responder.py](#) (Output)



```
kanamadisiddarth@Siddarth: $ python3 responder.py
Starting abuse responder with loaded YAML config...
[ALERT] Raw message: {"client_ip":"35.35.35.35","request_path":"/api","status":429,"latency":100,"timestamp":1690101130}
Offenses for 35.35.35.35: 1
[ALERT] Raw message: {"client_ip":"35.35.35.35","request_path":"/api","status":429,"latency":100,"timestamp":1690101130}
Offenses for 35.35.35.35: 2
[ALERT] Raw message: {"client_ip":"35.35.35.35","request_path":"/api","status":429,"latency":100,"timestamp":1690101130}
Offenses for 35.35.35.35: 3
[ALERT] Raw message: {"client_ip":"35.35.35.35","request_path":"/api","status":429,"latency":100,"timestamp":1690101130}
Offenses for 35.35.35.35: 4
[ALERT] Raw message: {"client_ip":"35.35.35.35","request_path":"/api","status":429,"latency":100,"timestamp":1690101130}
Offenses for 35.35.35.35: 5
Invalid log format:
[ALERT] Raw message: {"client_ip":"35.35.35.35","request_path":"/api","status":429,"latency":100,"timestamp":1690101130}
Offenses for 35.35.35.35: 6
[ALERT] Raw message: {"client_ip":"35.35.35.35","request_path":"/api","status":429,"latency":100,"timestamp":1690101130}
Offenses for 35.35.35.35: 7
[ALERT] Raw message: {"client_ip":"35.35.35.35","request_path":"/api","status":429,"latency":100,"timestamp":1690101130}
Offenses for 35.35.35.35: 8
[ALERT] Raw message: {"client_ip":"35.35.35.35","request_path":"/api","status":429,"latency":100,"timestamp":1690101130}
Offenses for 35.35.35.35: 9
```