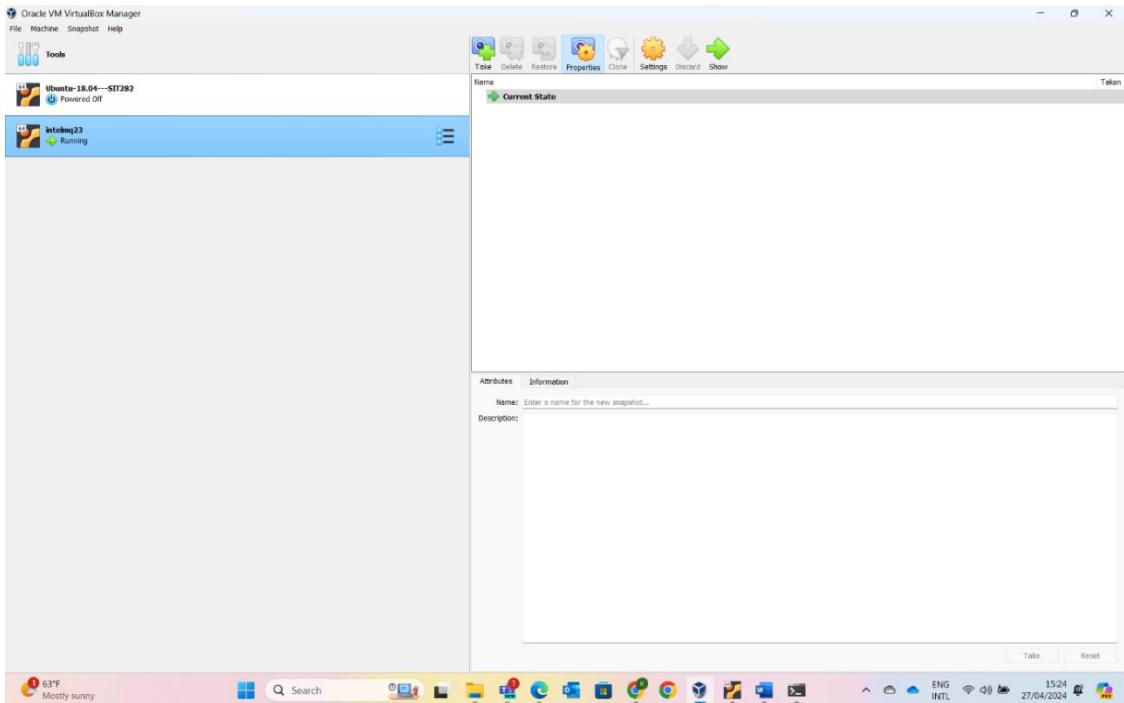


Integration of Intel MQ with an SQLite database.

Intel MQ installation and configuration:

Using the correct login credentials from Rads (username: intelapi, password: intelapi), I successfully accessed the IntelMQ user interface. Subsequently, I configured and managed various bots for diverse data outputs.



Access the server where IntelMQ is running. This can be done via SSH if you are working on a remote server.

```
ubuntu@ubuntu:~ % 
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

PS C:\Users\keert> ssh ubuntu@192.168.56.101
The authenticity of host '192.168.56.101 (192.168.56.101)' can't be established.
ED25519 key fingerprint is SHA256:druynepmZk+OMjsxC5bNFQt8YIa9IL510vqOeC/U7gY.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.56.101' (ED25519) to the list of known hosts.
ubuntu@192.168.56.101's password:
Welcome to Ubuntu 22.04.4 LTS (GNU/Linux 5.15.0-102-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/pro

 System information as of Sat Apr 27 05:10:30 AM UTC 2024

 System load:  0.3369140625   Processes:          170
 Usage of /:   40.6% of 23.70GB  Users logged in:   1
 Memory usage: 47%            IPv4 address for enp0s3: 10.0.2.15
 Swap usage:   0%             IPv4 address for enp0s8: 192.168.56.101

 Expanded Security Maintenance for Applications is not enabled.

 8 updates can be applied immediately.
 To see these additional updates run: apt list --upgradable

 9 additional security updates can be applied with ESM Apps.
 Learn more about enabling ESM Apps service at https://ubuntu.com/esm

 The list of available updates is more than a week old.
 To check for new updates run: sudo apt update

Last login: Sat Apr 27 04:54:33 2024
ubuntu@ubuntu:~$
```

```
* Documentation: https://help.ubuntu.com
* Management: https://landscape.canonical.com
* Support: https://ubuntu.com/pro

System information as of Sat Apr 27 05:16:14 AM UTC 2024

System load: 0.2275390625 Processes: 169
Usage of /: 40.6% of 23.70GB Users logged in: 1
Memory usage: 47% IPv4 address for enp0s3: 10.0.2.15
Swap usage: 0% IPv4 address for enp0s8: 192.168.56.101

Expanded Security Maintenance for Applications is not enabled.

8 updates can be applied immediately.
To see these additional updates run: apt list --upgradable

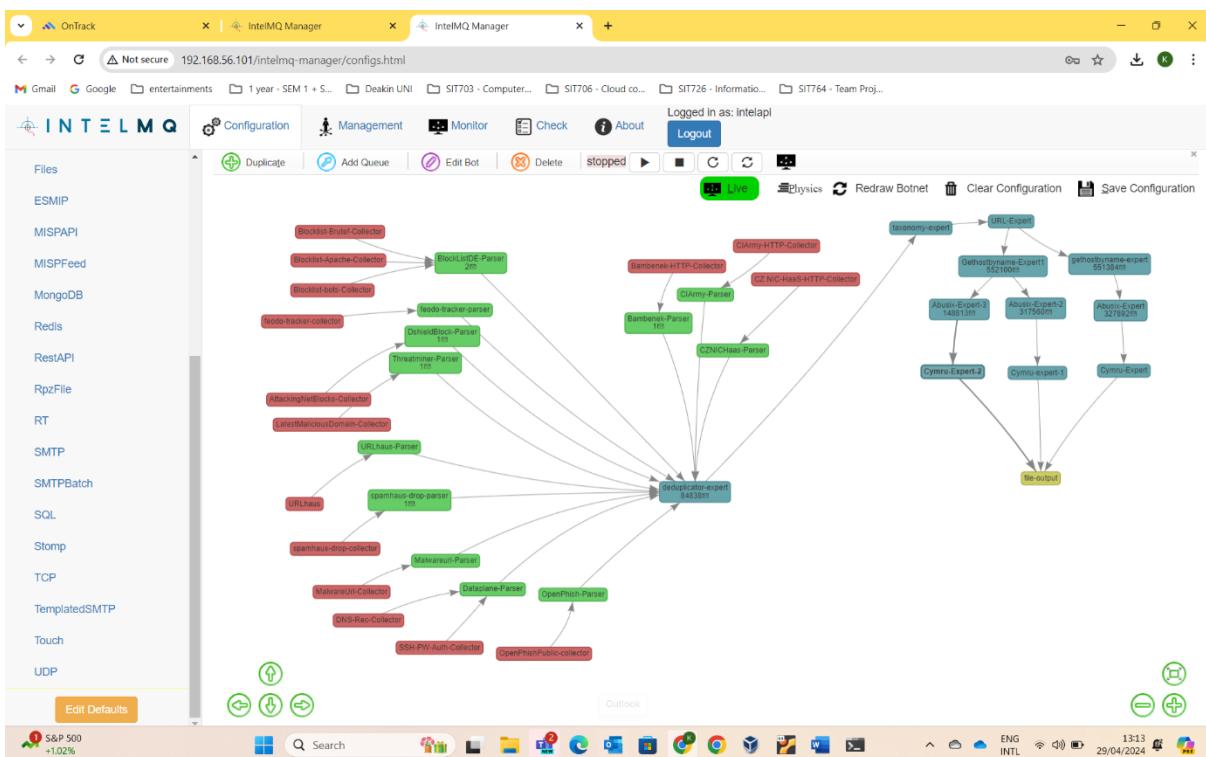
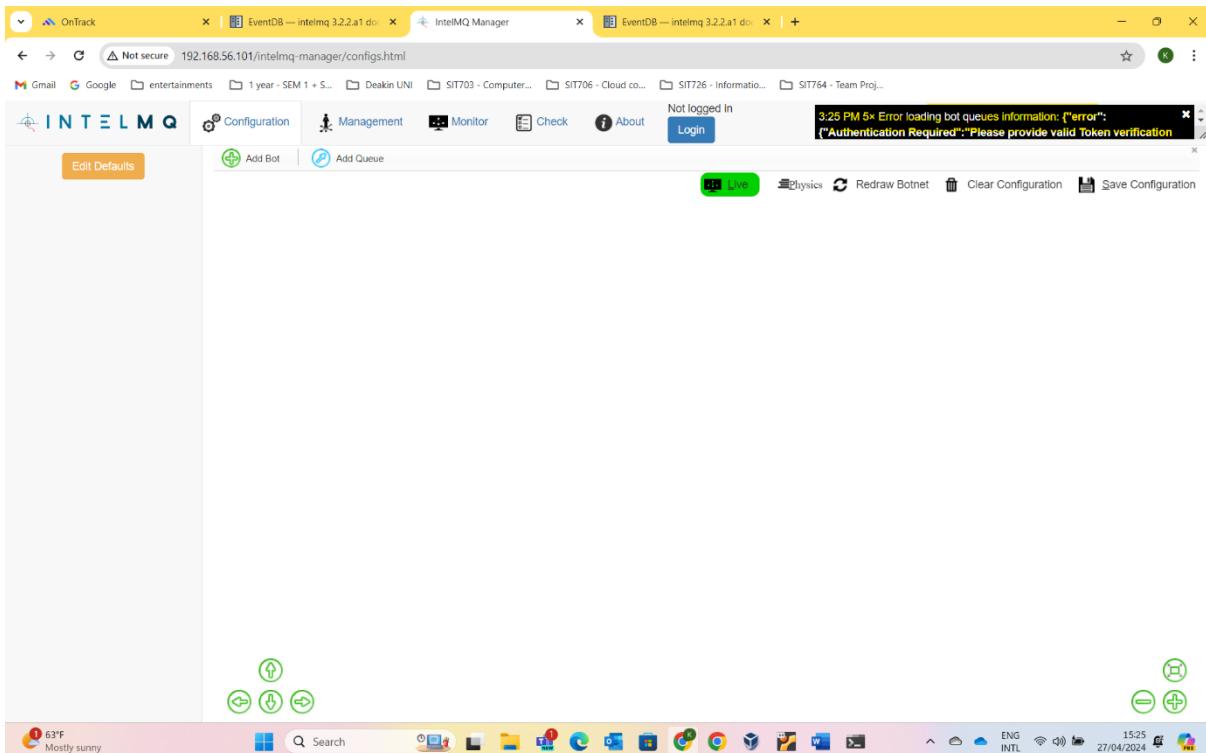
9 additional security updates can be applied with ESM Apps.
Learn more about enabling ESM Apps service at https://ubuntu.com/esm

The list of available updates is more than a week old.
To check for new updates run: sudo apt update

Last login: Sat Apr 27 05:10:31 2024 from 192.168.56.1
ubuntu@ubuntu:~$ cd /etc/intelmq
ubuntu@ubuntu:/etc/intelmq$ ls -la
total 96
drwxrwxr-x 3 intelmq intelmq 4096 Apr 21 13:16 .
drwxr-xr-x 103 root root 4096 Apr 12 06:58 ..
-rw-rw-r-- 1 intelmq intelmq 426 Mar 1 13:19 api-apache.conf
-rw-rw-r-- 1 intelmq intelmq 241 Mar 1 13:19 api-config.json
-rw-rw-r-- 1 intelmq intelmq 21099 Mar 1 13:19 harmonization.conf
drwxrwxr-x 2 intelmq intelmq 4096 Mar 28 00:48 manager
-rw-rw-r-- 1 intelmq intelmq 385 Mar 1 13:19 manager-apache.conf
-rw-rw-r-- 1 intelmq intelmq 22088 Apr 24 08:47 runtime.yaml
-rw-rw-r-- 1 intelmq intelmq 22043 Apr 24 08:47 runtime.yaml.bak
ubuntu@ubuntu:/etc/intelmq$ vi runtime.yaml
ubuntu@ubuntu:/etc/intelmq$ sudo intelmqctl status
[sudo] password for ubuntu:
Bot Abusix-Expert is stopped.
Bot Abusix-Expert-2 is stopped.
Bot Abusix-Expert-3 is stopped.
Bot AttackingNetBlocks-Collector is stopped.
Bot Bambenek-HTTP-Collector is stopped.
Bot Bambenek-Parser is stopped.

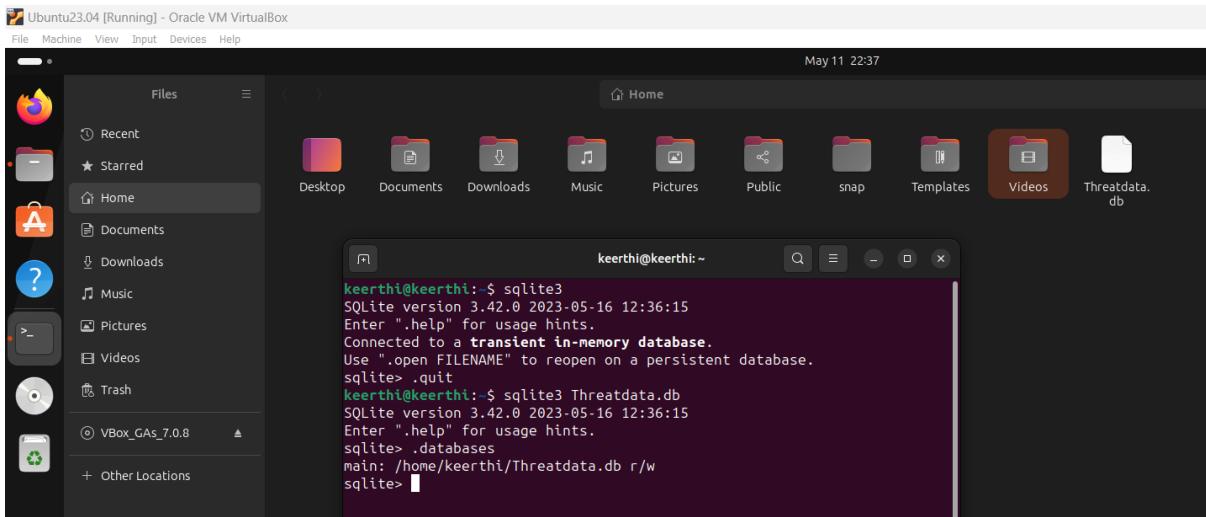
63°F Mostly sunny 15:23 27/04/2024 ENG INTL
```

```
-rw-rw-r-- 1 intelmq intelmq 22088 Apr 24 08:47 runtime.yaml
-rw-rw-r-- 1 intelmq intelmq 22043 Apr 24 08:47 runtime.yaml.bak
ubuntu@ubuntu:/etc/intelmq$ vi runtime.yaml
ubuntu@ubuntu:/etc/intelmq$ sudo intelmqctl status
[sudo] password for ubuntu:
Bot Abusix-Expert is stopped.
Bot Abusix-Expert-2 is stopped.
Bot Abusix-Expert-3 is stopped.
Bot AttackingNetBlocks-Collector is stopped.
Bot Bambenek-HTTP-Collector is stopped.
Bot Bambenek-Parser is stopped.
Bot BlockListDE-Parser is stopped.
Bot Blocklist-Apache-Collector is stopped.
Bot Blocklist-Brutef-Collector is stopped.
Bot Blocklist-bots-Collector is stopped.
Bot CIArmy-HTTP-Collector is stopped.
Bot CIArmy-Parser is stopped.
Bot CZ.NIC-HaaS-HTTP-Collector is stopped.
Bot CZNICHaas-Parser is stopped.
Bot Cymru-Expert is stopped.
Bot Cymru-Expert-2 is stopped.
Bot Cymru-expert-1 is stopped.
Bot DNS-Rec-Collector is stopped.
Bot DataPlane-Parser is stopped.
Bot DshieldBlock-Parser is stopped.
Bot Gethostbyname-Expert1 is stopped.
Bot LatestMaliciousDomain-Collector is stopped.
Bot MalwareUrl-Collector is stopped.
Bot Malwareurl-Parser is stopped.
Bot OpenPhish-Parser is stopped.
Bot OpenPhishPublic-collector is stopped.
Bot SSH-PW-Auth-Collector is stopped.
Bot Threatminer-Parser is stopped.
Bot URL-Expert is stopped.
Bot URLhaus is stopped.
Bot URLhaus-Parser is stopped.
Bot deduplicator-expert is stopped.
Bot feedo-tracker-collector is stopped.
Bot feedo-tracker-parser is stopped.
Bot file-output is stopped.
Bot gethostbyname-expert is stopped.
Bot spammhaus-drop-collector is stopped.
Bot spammhaus-drop-parser is stopped.
Bot taxonomy-expert is stopped.
ubuntu@ubuntu:/etc/intelmq$ ^C
ubuntu@ubuntu:/etc/intelmq$ ^C
ubuntu@ubuntu:/etc/intelmq$ |
```

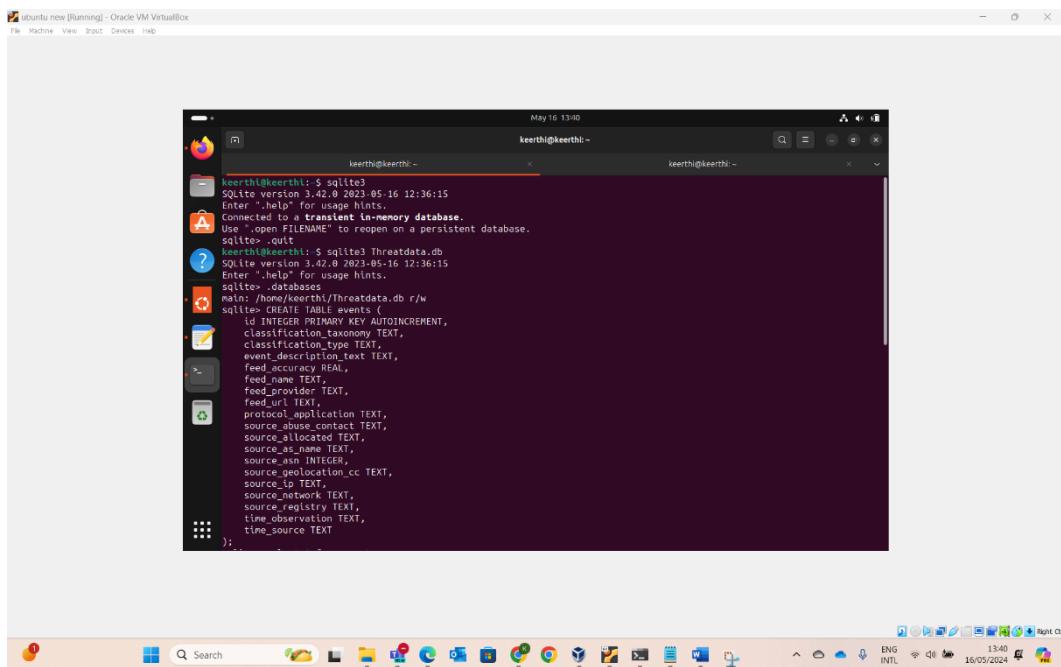


To facilitate data storage and management, I set up a dedicated Ubuntu virtual machine to host the SQLite3 database. Following the instructions outlined in the DigitalOcean tutorial:

<https://www.digitalocean.com/community/tutorials/how-to-install-and-use-sqlite-on-ubuntu-20-04>, I installed the SQLite3.



After completing the SQLite3 installation, I created a test database named Threatdata.db. Additionally, I created a new table called 'events' within the Threatdata.db database store the data. Testing connectivity between the IntelMQ instance and the Ubuntu VM hosting the database was successful, as confirmed by successful ping responses from both ends.



A screenshot of a Linux desktop environment, likely Ubuntu, running in Oracle VM VirtualBox. The desktop has a dark theme with a dock at the bottom containing icons for various applications like the Dash, Home, and Control Center. A terminal window titled 'keerthi@keerthi: ~' is open, showing a command-line session. The user runs 'sudo find / -type f -name "Threatdata.db"' and receives several errors: 'find: ./proc/628/task/7628/net': Invalid argument, 'find: ./proc/628/net': Invalid argument, 'find: /run/user/1000/gvfs': Permission denied, and 'find: /run/user/1000/doc': Permission denied. The terminal also shows '/home/keerthi/Threatdata.db' as the current directory. The desktop background is a solid dark color, and the overall interface is clean and modern.

```

ubuntu@ubuntu:/etc/intelmq$ ls
api-apache.conf api-config.json harmonization.conf manager manager-apache.conf runtime.yaml runtime.yaml.bak
ubuntu@ubuntu:/etc/intelmq$ nano runtime.yaml
ubuntu@ubuntu:/etc/intelmq$ cp runtime.yaml runtime_backup.yaml
cp: cannot create regular file 'runtime_backup.yaml': Permission denied
ubuntu@ubuntu:/etc/intelmq$ cp runtime.yaml runtime.bak
cp: cannot create regular file 'runtime.bak': Permission denied
ubuntu@ubuntu:/etc/intelmq$ cp runtime.yaml runtime_kp.yaml.bak
cp: cannot create regular file 'runtime_kp.yaml.bak': Permission denied
ubuntu@ubuntu:/etc/intelmq$ vi runtime.yaml
ubuntu@ubuntu:/etc/intelmq$ sudo cp runtime.yaml runtime.bak
[sudo] password for ubuntu:
ubuntu@ubuntu:/etc/intelmq$ ls
api-apache.conf api-config.json harmonization.conf manager manager-apache.conf runtime.bak runtime.yaml runtime.yaml.bak
ubuntu@ubuntu:/etc/intelmq$ sudo cp runtime.yaml runtime.yaml.bak
ubuntu@ubuntu:/etc/intelmq$ ls
api-apache.conf api-config.json harmonization.conf manager manager-apache.conf runtime.bak runtime.yaml runtime.yaml.bak
ubuntu@ubuntu:/etc/intelmq$ cd manager
ubuntu@ubuntu:/etc/intelmq/manager$ nano runtime.yaml
ubuntu@ubuntu:/etc/intelmq/manager$ ubuntu@ubuntu:/etc/intelmq/manager$ cd ..
ubuntu@ubuntu:/etc/intelmq$ nano runtime.yaml
ubuntu@ubuntu:/etc/intelmq$ nano runtime.yaml
ubuntu@ubuntu:/etc/intelmq$ nano runtime.yaml
ubuntu@ubuntu:/etc/intelmq$ nano runtime.yaml
ubuntu@ubuntu:/etc/intelmq$ ping 127.0.1.1
PING 127.0.1.1 (127.0.1.1) 56(84) bytes of data.
64 bytes from 127.0.1.1: icmp_seq=1 ttl=64 time=0.26 ms
64 bytes from 127.0.1.1: icmp_seq=2 ttl=64 time=0.063 ms
64 bytes from 127.0.1.1: icmp_seq=3 ttl=64 time=0.033 ms
64 bytes from 127.0.1.1: icmp_seq=4 ttl=64 time=0.034 ms
64 bytes from 127.0.1.1: icmp_seq=5 ttl=64 time=0.054 ms
64 bytes from 127.0.1.1: icmp_seq=6 ttl=64 time=0.027 ms
^C
--- 127.0.1.1 ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 5530ms
rtt min/avg/max/mdev = 0.027/0.912/5.262/1.945 ms
ubuntu@ubuntu:/etc/intelmq$
```

```

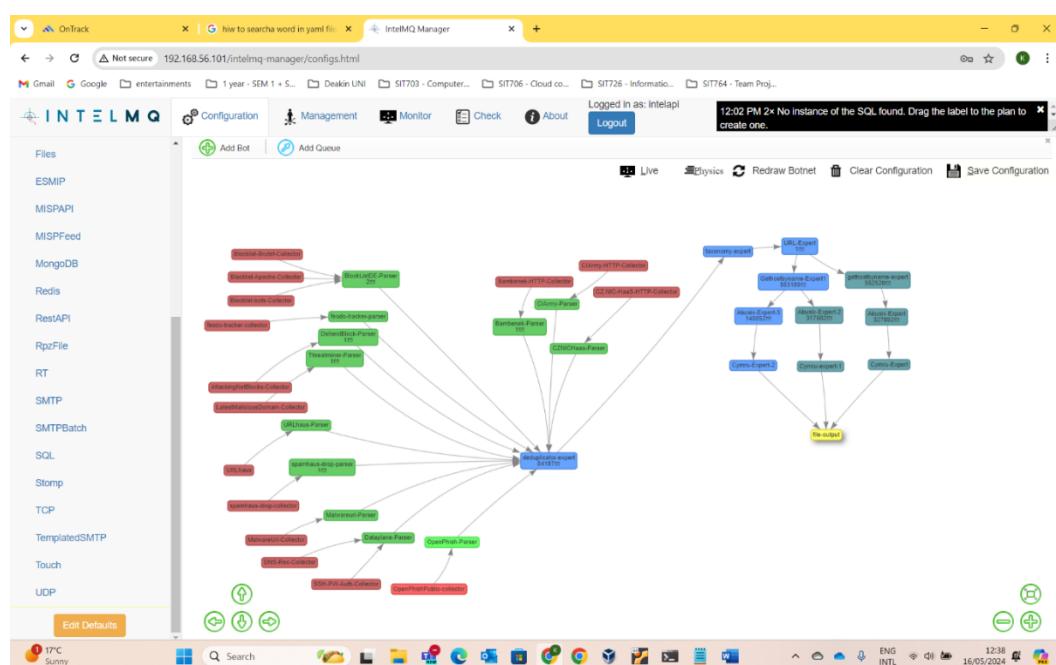
keerthi@keerthi:~$ ipconfig
Command 'ipconfig' not found, did you mean:
  command 'iwconfig' from deb wireless-tools (30-pre9-13.1ubuntu4)
  command 'lconfig' from deb ipmiutil (3.1.9-3)
  command 'lifconfig' from deb net-tools (2.10-0.1ubuntu3)
  command 'hipconfig' from deb hpc (5.2.3-12)
Try: sudo apt install <deb name>
keerthi@keerthi:~$ hostname -i
127.0.1.1
keerthi@keerthi:~$ sqlite3 /home/keerthi/Threatdata.db
SQLite version 3.42.0 2023-05-16 12:36:15
Enter ".help" for usage hints.
sqlite> .exit
keerthi@keerthi:~$ ping 192.168.56.101
PING 192.168.56.101 (192.168.56.101) 56(84) bytes of data.
64 bytes from 192.168.56.101: icmp_seq=1 ttl=63 time=5.01 ms
64 bytes from 192.168.56.101: icmp_seq=2 ttl=63 time=1.87 ms
64 bytes from 192.168.56.101: icmp_seq=3 ttl=63 time=1.45 ms
64 bytes from 192.168.56.101: icmp_seq=4 ttl=63 time=1.45 ms
64 bytes from 192.168.56.101: icmp_seq=5 ttl=63 time=2.51 ms
^C
... 192.168.56.101 ping statistics ...
5 packets transmitted, 5 received, 0% packet loss, time 4016ms
rtt min/avg/max/mdev = 1.448/2.458/5.006/1.331 ms
keerthi@keerthi:~$
```

Inserted dummy data into the events table I have created in the SQLite database Threatdata.db. This INSERT statement inserts one row of data into the events table with the specified values. we can modify the values as needed or execute this statement multiple times to insert multiple rows of dummy data. After inserting the data, we can query the events table to verify that the data has been successfully inserted using below command:

`SELECT * FROM events;`

This query will retrieve all rows from the events table, allowing us to view the inserted dummy data.

The screenshot shows a Linux desktop environment with a terminal window open. The terminal window title is 'keerthi@keerthi: ~'. The terminal content displays a SQL query being executed against a SQLite database named 'events'. The query inserts a new row into the 'events' table, which contains information about a login attempt. The log entry includes details such as source ASN, location, IP, network, registry, observation time, and source. It also specifies the event type as 'intrusion-attempts' and 'brute-force', and notes that the address has been seen attempting to log in using SSH password authentication. The terminal also shows the creation of a new table 'events' with columns 'id', 'class', and 'SELECT * from events'. The bottom of the terminal window shows the command 'sqlite>'. The desktop interface includes a taskbar at the bottom with icons for various applications like File Explorer, Mail, and a web browser. The system tray on the right shows the date (16/05/2024), time (15:05), and connectivity status.



Use a command-line text viewer or editor to read the content of the events.txt file.

Using cat: This command will display the entire content of the file. I have used below command to open the contents of the file - cat /var/lib/intelmq/bots/file-output/events.txt.

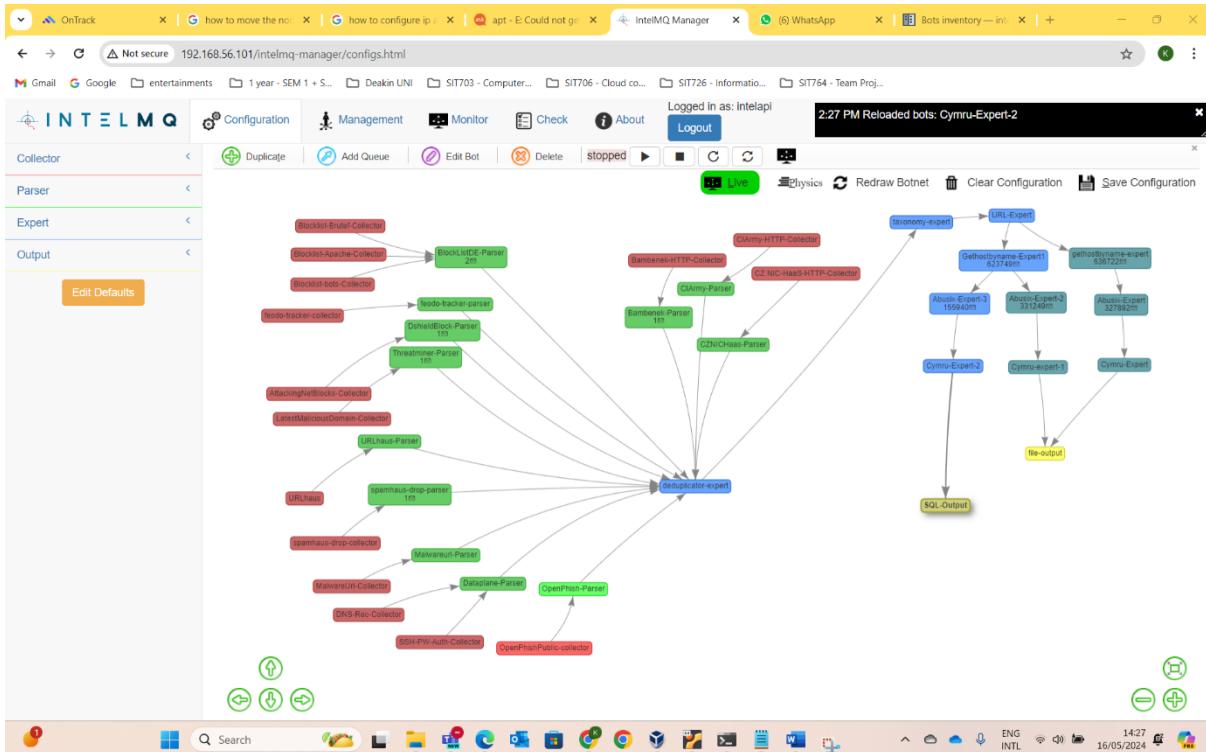
```
application": "ssh", "source.abuse_contact": "support@cnispgroup.com", "source.allocated": "2011-01-31T00:00:00+00:00", "source.as_name": "FASTIDC", "source.asn": "56005", "source.geolocation.cc": "CN", "source.ip": "42.51.48.229", "source.network": "42.51.0.0/18", "source.registry": "APNIC", "time.observation": "2024-04-13T18:41:46+00:00", "time.source": "2024-04-13T17:07:59+00:00"}, {"classification.taxonomy": "intrusion-attempts", "classification.type": "brute-force", "event.description.text": "Address has been seen attempting to remotely log in to a host using SSH password authentication. The source report lists hosts that are highly suspicious and are likely conducting malicious SSH pass word authentication attacks.", "feed.accuracy": 100.0, "feed.name": "HTTP", "feed.provider": "Dataplane", "feed.url": "https://dataplane.org/sshauth.txt", "protocol.application": "ssh", "source.abuse_contact": "abuse@chinamobile.com", "source.allocated": "2007-07-17T00:00:00+00:00", "source.as_name": "CMNET-Z HEJIANG-AP", "source.asn": "56084", "source.geolocation.cc": "CN", "source.ip": "117.148.166.174", "source.network": "117.148.166.0/24", "source.registry": "AP NIC", "time.observation": "2024-04-13T18:41:46+00:00", "time.source": "2024-04-13T17:59:45+00:00"}, {"classification.taxonomy": "intrusion-attempts", "classification.type": "brute-force", "event.description.text": "Address has been seen attempting to remotely log in to a host using SSH password authentication. The source report lists hosts that are highly suspicious and are likely conducting malicious SSH pass word authentication attacks.", "feed.accuracy": 100.0, "feed.name": "HTTP", "feed.provider": "Dataplane", "feed.url": "https://dataplane.org/sshauth.txt", "protocol.application": "ssh", "source.abuse_contact": "abuse@chinamobile.com", "source.allocated": "2009-11-08T00:00:00+00:00", "source.as_name": "CMNET-Z HEJIANG-AP", "source.asn": "56084", "source.geolocation.cc": "CN", "source.ip": "183.245.232.31", "source.network": "183.245.232.0/22", "source.registry": "AP NIC", "time.observation": "2024-04-13T18:41:46+00:00", "time.source": "2024-04-13T17:55:44+00:00"}, {"classification.taxonomy": "intrusion-attempts", "classification.type": "brute-force", "event.description.text": "Address has been seen attempting to remotely log in to a host using SSH password authentication. The source report lists hosts that are highly suspicious and are likely conducting malicious SSH pass word authentication attacks.", "feed.accuracy": 100.0, "feed.name": "HTTP", "feed.provider": "Dataplane", "feed.url": "https://dataplane.org/sshauth.txt", "protocol.application": "ssh", "source.abuse_contact": "abuse@chinamobile.com", "source.allocated": "2011-01-24T00:00:00+00:00", "source.as_name": "CMNET-Z HEJIANG-AP", "source.asn": "56084", "source.geolocation.cc": "CN", "source.ip": "36.138.130.222", "source.network": "36.138.130.0/23", "source.registry": "AP NIC", "time.observation": "2024-04-13T18:41:46+00:00", "time.source": "2024-04-13T17:59:35+00:00"}, {"classification.taxonomy": "intrusion-attempts", "classification.type": "brute-force", "event.description.text": "Address has been seen attempting to remotely log in to a host using SSH password authentication. The source report lists hosts that are highly suspicious and are likely conducting malicious SSH pass word authentication attacks.", "feed.accuracy": 100.0, "feed.name": "HTTP", "feed.provider": "Dataplane", "feed.url": "https://dataplane.org/sshauth.txt", "protocol.application": "ssh", "source.abuse_contact": "abuse@chinamobile.com", "source.allocated": "2011-01-24T00:00:00+00:00", "source.as_name": "CMNET-Z HEJIANG-AP", "source.asn": "56084", "source.geolocation.cc": "CN", "source.ip": "36.139.89.196", "source.network": "36.139.88.0/21", "source.registry": "APNIC", "time.observation": "2024-04-13T18:41:46+00:00", "time.source": "2024-04-13T17:56:13+00:00"}, {"classification.taxonomy": "intrusion-attempts", "classification.type": "brute-force", "event.description.text": "Address has been seen attempting to remotely log in to a host using SSH password authentication. The source report lists hosts that are highly suspicious and are likely conducting malicious SSH pass word authentication attacks.", "feed.accuracy": 100.0, "feed.name": "HTTP", "feed.provider": "Dataplane", "feed.url": "https://dataplane.org/sshauth.txt", "protocol.application": "ssh", "source.abuse_contact": "abuse@chinamobile.com", "source.allocated": "2011-04-01T00:00:00+00:00", "source.as_name": "CMNET-Z HANXI-AP", "source.asn": "56084", "source.geolocation.cc": "CN", "source.ip": "39.174.90.19", "source.network": "39.174.64.0/19", "source.registry": "APNIC", "time.observation": "2024-04-13T18:41:46+00:00", "time.source": "2024-04-13T17:34:13+00:00"}, {"classification.taxonomy": "intrusion-attempts", "classification.type": "brute-force", "event.description.text": "Address has been seen attempting to remotely log in to a host using SSH password authentication. The source report lists hosts that are highly suspicious and are likely conducting malicious SSH pass word authentication attacks.", "feed.accuracy": 100.0, "feed.name": "HTTP", "feed.provider": "Dataplane", "feed.url": "https://dataplane.org/sshauth.txt", "protocol.application": "ssh", "source.abuse_contact": "abuse@chinamobile.com", "source.allocated": "2009-05-06T00:00:00+00:00", "source.as_name": "CMNET-S JIANGSU-ADP", "source.asn": "56084", "source.geolocation.cc": "CN", "source.ip": "111.53.104.249", "source.network": "111.53.0.0/16", "source.registry": "APNIC", "time.observation": "2024-04-13T18:41:46+00:00", "time.source": "2024-04-13T17:47:24+00:00"}, {"classification.taxonomy": "intrusion-attempts", "classification.type": "brute-force", "event.description.text": "Address has been seen attempting to remotely log in to a host using SSH password authentication. The source report lists hosts that are highly suspicious and are likely conducting malicious SSH pass word authentication attacks.", "feed.accuracy": 100.0, "feed.name": "HTTP", "feed.provider": "Dataplane", "feed.url": "https://dataplane.org/sshauth.txt", "protocol.application": "ssh", "source.abuse_contact": "abuse@chinamobile.com", "source.allocated": "2010-07-01T00:00:00+00:00", "source.as_name": "CMNET-J JIANGSU-ADP", "source.asn": "56084", "source.geolocation.cc": "CN", "source.ip": "223.68.169.181", "source.network": "223.68.168.0/22", "source.registry": "APNIC", "time.observation": "2024-04-13T18:41:46+00:00", "time.source": "2024-04-13T17:12:21+00:00"}, {"classification.taxonomy": "intrusion-attempts", "classification.type": "brute-force", "event.description.text": "Address has been seen attempting to remotely log in to a host using SSH password authentication. The source report lists hosts that are highly suspicious and are likely conducting malicious SSH pass word authentication attacks.", "feed.accuracy": 100.0, "feed.name": "HTTP", "feed.provider": "Dataplane", "feed.url": "https://dataplane.org/sshauth.txt", "protocol.application": "ssh", "source.abuse_contact": "abuse@chinamobile.com", "source.allocated": "2011-01-01T00:00:00+00:00", "source.as_name": "CMNET-Z HUANGHE-ADP", "source.asn": "56084", "source.geolocation.cc": "CN", "source.ip": "223.68.169.181", "source.network": "223.68.168.0/22", "source.registry": "APNIC", "time.observation": "2024-04-13T18:41:46+00:00", "time.source": "2024-04-13T17:12:21+00:00"}]
```

In the IntelMQ configuration file located at /etc/intelmq/runtime.yaml, I attempted to define an output section for the SQL output bot named SQLiteOutput. However, a permission denied error was encountered due to insufficient write permissions for the file.

```
ubuntu@ubuntu:/etc/intelmq    +   
GNU nano 6.2                      runtime.yaml *  
  
http_password: ''  
http_url: https://feodotracker.abuse.ch/downloads/ipblocklist.json  
http_url_formatting: false  
http_username: ''  
name: Feodo Tracker  
provider: Abuse.ch  
rate_limit: 86400  
ssl_client_certificate: ::  
run_mode: continuous  
feodo-tracker-parser:  
bot_id: feodo-tracker-parser  
description: Parser for Feodo Tracker collector.  
enabled: true  
group: Parser  
groupname: parsers  
module: intelmq.bots.parsers.abusech.parser_feodotracker  
name: Feodo Tracker Parser  
parameters:  
destination_queues:  
_default: [deduplicator-expert-queue]  
run_mode: continuous  
SQLiteOutput:  
bot_id: sqlite-output  
description: Store events in SQLite database  
enabled: true  
group: Output  
groupname: outputs  
module: intelmq.bots.outputs.sqlite.output  
parameters:  
database: /home/keerthi/Threatdata.db  
table: events  
run_mode: continuous  
gethostbyname-expert:  
bot_id: gethostbyname-expert  
description: fqdn2ip is the bot responsible to parsing the ip from the fqdn.  
enabled: true  
group: Expert  
groupname: experts  
module: intelmq.bots.experts.gethostbyname.expert  
name: Gethostbyname  
parameters:  
destination_queues:  
_default: [Abusix-Expert-queue]  
[ Error writing runtime.yaml: Permission denied ]  
File Help   ^W Write Out   ^A Where Is   ^K Cut   ^E Execute   ^C Location   M-U Undo  
^X Exit   ^R Read File   ^W Replace   ^P Paste   ^J Execute   ^G Go To Line   M-E Redo  
M-A Set Mark   M-T To Bracket  
M-Q Where Was  
ENG INTL 14:00 16/05/2024
```

To circumvent the permission issue, I configured the SQL-Output bot through the IntelMQ user interface in Intelmq-Manager. I integrated the bot into the workflow by dragging it and attaching it downstream of the parser component. Subsequently, I configured the necessary parameters such as description, database path(/home/keerthi/Threatdata.db), host (set to 127.0.1.1), table name, and user credentials.

```
ubuntu@ubuntu:/etc/intelmq$ nano runtime.yaml
parameters:
  bottype: Collector
  code: ''
  destination_queues:
    _default: [OpenPhish-Parser-queue]
  documentation: ''
  extract_files: false
  gpg_keyring: ''
  http_header: {}
  http_password: ''
  http_url: https://www.openphish.com/feed.txt
  http_url_formatting: false
  http_username: ''
  provider: OpenPhish
  rate_limit: 86400
  signature_url: ''
  signature_url_formatting: false
  ssl_client_cert: ''
  ssl_client_certificate: ''
  verify_pgp_signatures: false
  run_mode: continuous
SQL-Output:
  bot_id: SQL-Output
  description: Send events to a SQLite database
  enabled: true
  group: Output
  module: intelmq.bots.outputs.sql.output
  name: SQL
  parameters:
    autocommit: true
    bottype: Output
    database: /home/keerthi/Threatdata.db
    destination_queues: {}
    engine: ''
    fail_on_errors: false
    fields: ''
    host: 127.0.1.1
    jsondict_as_string: true
    message_jsondict_as_string: true
    password: ''
    port: 5432
    reconnect_delay: 0
    sslmode: require
```



Upon initiating the execution of the configured bots to process the data flow, the expected output was not generated as anticipated. Further investigation and troubleshooting are required to identify and address the underlying cause of this discrepancy. I did some trouble shooting to find the issue:

Checking Configuration: I double-checked the configuration I set up in the UI to ensure that the database path, host, table name, user, and all other relevant settings were correctly entered.

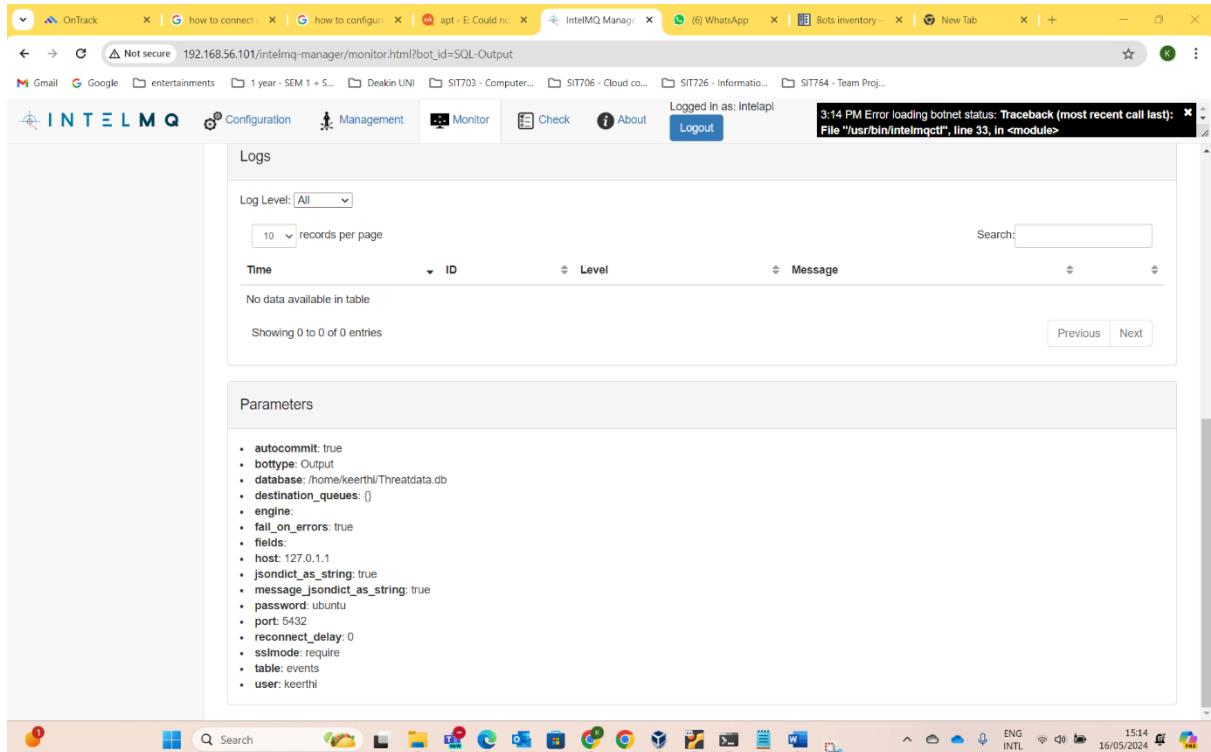
Database Connection: I verified that the SQLite database is accessible from the host where IntelMQ is running. I ensured there were no firewall rules or other network issues blocking the connection.

Bot Logs: Unfortunately, I couldn't find any logs for the SQL-Output bot. Checking the logs of the bot for any errors or warnings could provide valuable insight into what might be going wrong.

Data Flow: Due to being new to IntelMQ, I faced challenges in checking the data flow. It's essential to ensure that the data is being processed and passed to the SQL-Output bot correctly from preceding stages like parsers. Any issues upstream could prevent data from reaching the output bot.

Permissions: I observed that when I configured the output bot in IntelMQ Manager, the runtime.yaml file created the SQL-output bot with all the parameters I provided. Ensuring that the user running IntelMQ has the necessary permissions to write to the SQLite database file and access the specified table is crucial.

Restarting IntelMQ: I attempted to restart IntelMQ, as sometimes changes made in the UI may require a restart for them to take effect. Ensuring that I restarted IntelMQ after making the configuration changes was part of my trouble shooting process.



I was not able to see any log information and there is no output generated even after all that troubleshooting I was not able to fix the issue by myself.

Findings from the Intel MQ and SQL Database Integration task:

Successes:

Access to Intel MQ Interface: Successfully accessed the Intel MQ user interface using provided credentials.

Bot Configuration: Configured and managed various bots for data outputs within the Intel MQ environment.

SQLite Installation: Installed SQLite3 on a dedicated Ubuntu virtual machine to serve as the database backend.

Database Setup: Created a test database named Threatdata.db and initialized a table named 'events' within it for data storage.

Connectivity Establishment: Successfully established ping connectivity between the Intel MQ instance and the dedicated Ubuntu VM.

Bot Integration: Configured the SQL-Output bot through the Intel MQ user interface, specifying necessary parameters such as description, database path, host, table name, and user credentials.

Challenges:

Permission Error: Encountered a permission denied error while attempting to define the output section for the SQL-Output bot in the runtime.yaml file, indicating insufficient write permissions.

Output Discrepancy: Despite configuring the bots, initiating their execution did not generate the expected output as anticipated.

Troubleshooting Steps:

Configuration Verification: Confirmed the accuracy of configuration settings including database path, host, table name, and user credentials.

Accessibility Check: Ensured accessibility of the SQLite database from the Intel MQ host by ruling out firewall or network issues.

Log Examination: Attempted to retrieve logs from the SQL-Output bot for insights, unfortunately, logs were not available.

Data Flow Inspection: Investigated the data flow to confirm data transmission to the output bot.

Permissions Review: Reviewed user permissions for the Intel MQ process to access and write to the database file.

System Restart: Restarted IntelMQ to enforce configuration changes.

Unresolved Issue: Despite diligent troubleshooting efforts, the expected output from the SQL-Output bot remains elusive. The absence of logs from the bot complicates further investigation.

Next Steps:

Thorough Investigation: Need thorough investigation to pinpoint the root cause of why the SQL-Output bot fails to generate output with seniors/experts to gain insights and perspectives on resolving the issue efficiently.

References:

- [1] DigitalOcean, "How To Install and Use SQLite on Ubuntu 20.04," DigitalOcean, 23 July 2020. [Online]. Available: <https://www.digitalocean.com/community/tutorials/how-to-install-and-use-sqlite-on-ubuntu-20-04>. [Accessed: 17-May-2024].
- [2] IntelMQ Team, "EventDB — IntelMQ 3.0.0 documentation," IntelMQ, 2024. [Online]. Available: <https://intelmq.readthedocs.io/en/develop/user/eventdb.html>. [Accessed: 17-May-2024].
- [3] IntelMQ Team, "IntelMQ Tutorial: Lesson 3," GitHub, 2024. [Online]. Available: <https://github.com/certtools/intelmq-tutorial/blob/master/lesson-3.md>. [Accessed: 17-May-2024].
- [4] IntelMQ Team, "intelmq/bots/outputs at develop," GitHub, 2024. [Online]. Available: <https://github.com/certtools/intelmq/tree/develop/intelmq/bots/outputs>. [Accessed: 17-May-2024].
- [5] A. Kaplan, "IntelMQ: A Framework for CERTs for Collecting and Processing Security Feeds," FIRST, 2020. [Online]. Available: <https://www.first.org/resources/papers/malaga20/PUBLIC-Aaron-Kaplan-IntelMQ-malaga-20200131.pdf>. [Accessed: 17-May-2024].