

## 31. GIẢI PHÁP-TESTING - Task #1222

Task # 1211 (Closed): Cài đặt server log tập trung

### Setup mail server axigen lab test

30-09-2024 11:22 - Minh Pham

<b>Trạng thái:</b>	Closed	<b>Bắt đầu:</b>	22-09-2024
<b>Mức ưu tiên:</b>	Normal	<b>Hết hạn:</b>	30-09-2024
<b>Phân công cho:</b>	Minh Pham	<b>Tiến độ:</b>	0%
<b>Chủ đề:</b>		<b>Thời gian ước lượng:</b>	0:00 giờ
<b>Phiên bản:</b>		<b>Thời gian:</b>	0:00 giờ

#### Mô tả

Mục tiêu:

Setup server mail axigen để gửi log về server elasticsearch

Kết quả thực hiện:

Setup server mail lab

```
root@ubuntu:~# systemctl status fluent-bit.service
● fluent-bit.service - Fluent Bit
   Loaded: loaded (/lib/systemd/system/fluent-bit.service; disabled; vendor preset: enabled)
   Active: active (running) since Mon 2024-09-30 02:48:26 UTC; 4h 53min ago
     Docs: https://docs.fluentbit.io/manual/
  Main PID: 8993 (fluent-bit)
    Tasks: 5 (limit: 9423)
   Memory: 6.4M
   CGroup: /system.slice/fluent-bit.service
           └─8993 /opt/fluent-bit/bin/fluent-bit -c //etc/fluent-bit/fluent-bit.conf

Sep 30 02:48:26 ubuntu fluent-bit[8993]: [2024/09/30 02:48:26] [ info] [input:tail:tail.0] initializing
Sep 30 02:48:26 ubuntu fluent-bit[8993]: [2024/09/30 02:48:26] [ info] [input:tail:tail.0] storage_strategy=
Sep 30 02:48:26 ubuntu fluent-bit[8993]: [2024/09/30 02:48:26] [ info] [input:tail:tail.0] db: delete unmoni
Sep 30 02:48:26 ubuntu fluent-bit[8993]: [2024/09/30 02:48:26] [ info] [input:tail:tail.1] initializing
Sep 30 02:48:26 ubuntu fluent-bit[8993]: [2024/09/30 02:48:26] [ info] [input:tail:tail.1] storage_strategy=
Sep 30 02:48:26 ubuntu fluent-bit[8993]: [2024/09/30 02:48:26] [ info] [input:tail:tail.1] db: delete unmoni
Sep 30 02:48:26 ubuntu fluent-bit[8993]: [2024/09/30 02:48:26] [ info] [sp] stream processor started
Sep 30 02:48:26 ubuntu fluent-bit[8993]: [2024/09/30 02:48:26] [ info] [output:es:es.0] worker #0 started
Sep 30 02:48:26 ubuntu fluent-bit[8993]: [2024/09/30 02:48:26] [ info] [output:es:es.0] worker #1 started
Sep 30 02:48:26 ubuntu fluent-bit[8993]: [2024/09/30 02:48:26] [ info] [input:tail:tail.0] inotify_fs_add():
```

```

[SERVICE]
Parsers_File /etc/fluent-bit/parsers.conf
Parsers_File /etc/fluent-bit/axigen_parser.conf
Flush 10

[INPUT]
Name tail
Path /var/opt/axigen/log/default.txt
Tag axi.everything
Mem_Buf_Limit 50M
DB /var/opt/axigen/log/fluent-bit.db
Refresh_Interval 10

[FILTER]
Name parser
Match axi.everything
Key_Name log
Parser axi.everything_parser

[FILTER]
Name modify
Match axi.everything
Add tag axi.everything

[INPUT]
Name tail
Path /var/opt/axigen/log/security.txt
Tag axi.security
Mem_Buf_Limit 50M
DB /var/opt/axigen/log/fluent-bit.db
Refresh_Interval 10

[FILTER]
Name parser
Match axi.security
Key_Name log
Parser axi.security_parser

[FILTER]
Name modify
Match axi.security
Add tag axi.security

[OUTPUT]
Name es
Host 192.168.69.196
Index search
Port 9200
# If the Elasticsearch endpoint is secure (SSL / TLS), uncomment the line below
# tls On
# If a self-signed certificate is used, certificate validation should be disabled
# tls.verify Off

```

View Log Files

[Logged in as admin on ubuntu](#)
[CONTACT SUPPORT](#)
[LOG OUT](#)

- Acceptance & Routing
- Incoming Message Rules
- View Quarantine
- UPGRADES & UPDATES
- QUEUE
- Processing
- View Queue
- STATUS & MONITORING
- Reporting Service
- Charts
- Storage Charts
- LOGGING
- Local Services Log
- Log Collection Rules
- View Log Files
- Log Server Settings
- BACK-UP & RESTORE
- FTP Back-up & Restore
- File System Access
- AUTOMATIC MIGRATION
- CLUSTERING
- Clustering Setup

#	FILE NAME	LAST CHANGED	SIZE	ACTIONS
1	fluent-bit.db-wal	Mon, 30 Sep 2024 03:05:42	1 MB	<a href="#">VIEW</a> <a href="#">DELETE</a> <a href="#">DOWNLOAD LOG FILE</a>
2	default.txt	Mon, 30 Sep 2024 03:05:42	119 KB	<a href="#">VIEW</a> <a href="#">DELETE</a> <a href="#">DOWNLOAD LOG FILE</a>
3	fluent-bit.db-shm	Mon, 30 Sep 2024 03:05:38	32 KB	<a href="#">VIEW</a> <a href="#">DELETE</a> <a href="#">DOWNLOAD LOG FILE</a>
4	fluent-bit.db	Mon, 30 Sep 2024 02:48:26	8 KB	<a href="#">VIEW</a> <a href="#">DELETE</a> <a href="#">DOWNLOAD LOG FILE</a>

View Log File: default.txt

```

# created by AXIGEN version 10.5.26
2024-09-30 02:27:49 +0000 08 ubuntu PROCESSING:00000000: Shepherd thread is started
2024-09-30 02:27:49 +0000 08 ubuntu PROCESSING:00000000: Queue directory /var/opt/axigen/queue// scan complete: 0 mails found; current queue size: 0
2024-09-30 02:28:09 +0000 08 ubuntu JOBLOG:70000000: LetsE: Acme job executing
2024-09-30 02:28:09 +0000 08 ubuntu JOBLOG:70000000: LetsE: No cli jobs or renewals to do, going to sleep
2024-09-30 02:28:49 +0000 08 ubuntu PROCESSING:0032D402: Shepherd thread received signal for processing
2024-09-30 02:28:49 +0000 08 ubuntu PROCESSING:0032D402: Set recipient (postmaster@localdomain) state to RECEIVED
2024-09-30 02:28:49 +0000 08 ubuntu PROCESSING:0032D402: Set recipient (statistics@axigen.com) state to RECEIVED
2024-09-30 02:28:49 +0000 08 ubuntu PROCESSING:0032D402: Set mail state to PROCESSING
2024-09-30 02:28:49 +0000 08 ubuntu PROCESSING:0032D402: Start processing mail
2024-09-30 02:28:49 +0000 08 ubuntu PROCESSING:0032D402: Processing started
2024-09-30 02:28:49 +0000 08 ubuntu PROCESSING:0032D402: Filter AXI-TNEF loaded from file /opt/axigen/afsl/axi-tnef.afsl
2024-09-30 02:28:49 +0000 08 ubuntu PROCESSING:0032D402: Set recipient (postmaster@localdomain) state to PROCESSING
2024-09-30 02:28:49 +0000 08 ubuntu PROCESSING:0032D402: Start filter smtp routing
2024-09-30 02:28:49 +0000 08 ubuntu PROCESSING:0032D402: Processing started
2024-09-30 02:28:49 +0000 08 ubuntu PROCESSING:0032D402: Shepherd thread finished processing signal
2024-09-30 02:28:49 +0000 08 ubuntu PROCESSING:0032D402: No certificate loaded; disabling STARTTLS
2024-09-30 02:28:49 +0000 08 ubuntu PROCESSING:0032D402: Greylist enabled
2024-09-30 02:28:49 +0000 08 ubuntu PROCESSING:0032D402: Set max data size to 10240 KB

```

## Config log mail to elk

```
> Sep 30, 2024 @ 09:57:39.000 @timestamp: Sep 30, 2024 @ 09:57:39.000 host: ubuntu jobID: 00000014 log: <ff31cfa370c57e1f292076f1d9ffb7ed> GET /?_h=da87bc4c58ef9456dcf50c59bf28d4c8&page=v1f&action=edit&fileName=default%252etxt HTTP/1.1 u=admin code=200 time=20 logLevel: 08 service: WEBADMIN tag: axi.everything _id: fAjcQJIBif0Qt_aC0tzt _index: search _score: - _type: _doc

> Sep 30, 2024 @ 09:57:39.000 @timestamp: Sep 30, 2024 @ 09:57:39.000 host: ubuntu jobID: 00000014 log: <ff31cfa370c57e1f292076f1d9ffb7ed> GET /sources/logging/page_log_file_content.hsp?_h=da87bc4c58ef9456dcf50c59bf28d4c8&fileName=default%2etxt HTTP/1.1 u=admin code=200 time=2 logLevel: 08 service: WEBADMIN tag: axi.everything _id: f0jcQJIBif0Qt_aC0tzt _index: search _score: - _type: _doc

> Sep 30, 2024 @ 09:57:36.000 @timestamp: Sep 30, 2024 @ 09:57:36.000 host: ubuntu jobID: 00000014 log: <ff31cfa370c57e1f292076f1d9ffb7ed> GET /?_h=da87bc4c58ef9456dcf50c59bf28d4c8&page=v1f HTTP/1.1 u=admin code=200 time=24 logLevel: 08 service: WEBADMIN tag: axi.everything _id: GgjcQJIBif0Qt_aCq9zd _index: search _score: - _type: _doc

> Sep 30, 2024 @ 09:57:34.000 @timestamp: Sep 30, 2024 @ 09:57:34.000 host: ubuntu jobID: 00000014 log: <ff31cfa370c57e1f292076f1d9ffb7ed> GET /?_h=da87bc4c58ef9456dcf50c59bf28d4c8&page=rlc HTTP/1.1 u=admin code=200 time=14 logLevel: 08 service: WEBADMIN tag: axi.everything _id: G0jcQJIBif0Qt_aCq9zd _index: search _score: - _type: _doc

> Sep 30, 2024 @ 09:57:19.000 @timestamp: Sep 30, 2024 @ 09:57:19.000 host: ubuntu jobID: 00000014 log: <ff31cfa370c57e1f292076f1d9ffb7ed> GET /?_h=da87bc4c58ef9456dcf50c59bf28d4c8&page=1lo HTTP/1.1 u=admin code=200 time=30 logLevel: 08 service: WEBADMIN tag: axi.everything _id: cAjcQJIBif0Qt_aChNvN _index: search _score: - _type: _doc

> Sep 30, 2024 @ 09:57:14.000 @timestamp: Sep 30, 2024 @ 09:57:14.000 host: ubuntu jobID: 00000014 log: <ff31cfa370c57e1f292076f1d9ffb7ed> GET /?_h=da87bc4c58ef9456dcf50c59bf28d4c8&page=rlced&action=view&priority=1000 HTTP/1.1 u=admin code=200 time=25 logLevel: 08 service: WEBADMIN tag: axi.everything _id: HAJcQJIBif0Qt_aCXdu- _index: search _score: - _type: _doc

> Sep 30, 2024 @ 09:57:12.000 @timestamp: Sep 30, 2024 @ 09:57:12.000 host: ubuntu jobID: 00000014 log: <ff31cfa370c57e1f292076f1d9ffb7ed> GET /?_h=da87bc4c58ef9456dcf50c59bf28d4c8&page=rlc HTTP/1.1 u=admin
```

## Lược sử

### #1 - 30-09-2024 14:37 - Minh Pham

- Tập tin clipboard-202409301435-jwslf.png được thêm
- Tập tin clipboard-202409301437-fzqth.png được thêm
- Mô tả cập nhật

### #2 - 30-09-2024 14:38 - Minh Pham

- Trạng thái thay đổi từ In Progress tới Closed

### #3 - 30-09-2024 18:30 - Minh Pham

- Tập tin clipboard-202409301830-yqfhw.png được thêm
- Tập tin clipboard-202409301830-2aovr.png được thêm
- Mô tả cập nhật

### #4 - 30-09-2024 18:31 - Minh Pham

- Mô tả cập nhật

## Tập tin

clipboard-202409301435-jwslf.png	159 KB	30-09-2024	Minh Pham
clipboard-202409301437-fzqth.png	225 KB	30-09-2024	Minh Pham
clipboard-202409301830-yqfhw.png	42,3 KB	30-09-2024	Minh Pham
clipboard-202409301830-2aovr.png	42,6 KB	30-09-2024	Minh Pham