31. GIẢI PHÁP-TESTING - Task #1398

Task # 1396 (Closed): Setup cluster elasticsearch trên DC

Setup log mail về elasticsearch

23-12-2024 10:06 - Minh Pham

Trạng thái:	Closed	**Bắt đầu:**	30-12-2024
Mức ưu tiên:	Normal	**Hết hạn:**	07-01-2025
Phân công cho:	Minh Pham	**Tiến độ:**	0%
Chủ đề:		**Thời gian ước lượng:**	0:00 giờ
Phiên bản:		**Thời gian:**	0:00 giờ

Mô tả

Mục tiêu : Setup log mail về elasticsearch

Kết quả thực hiện:

Setup fluent bit đẩy log mail về elasticsearch

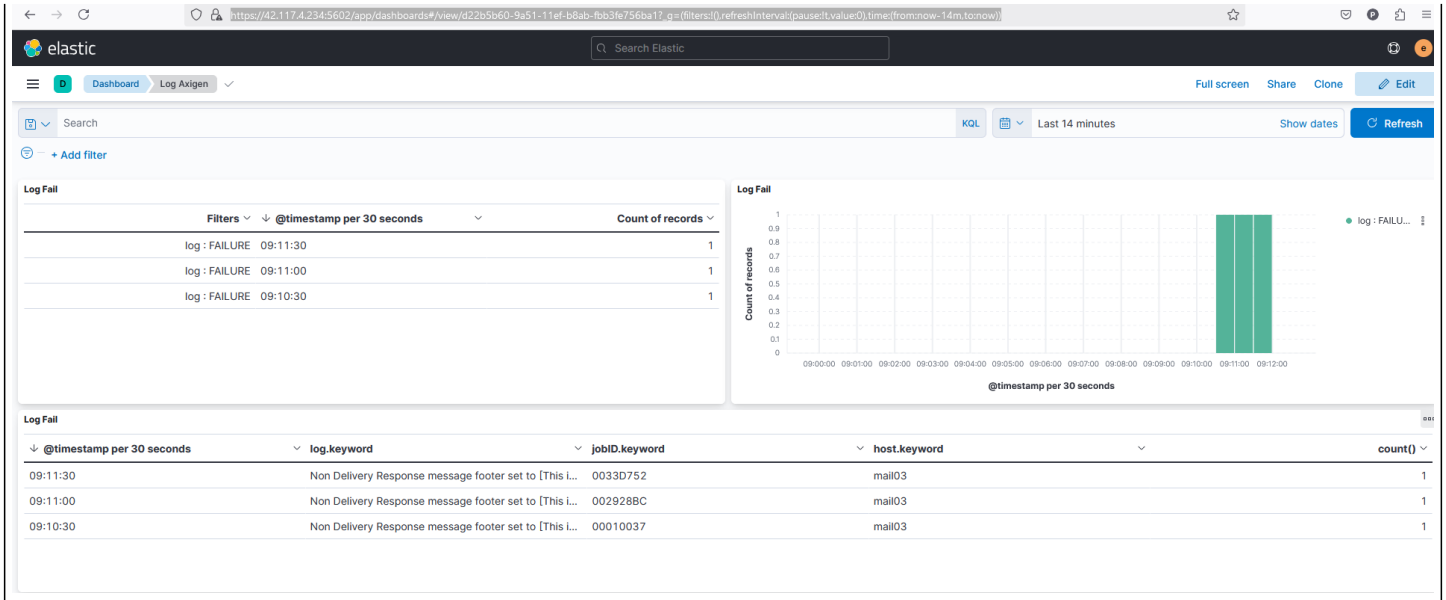
```
root@Server:~# systemctl status fluent-bit.service
● fluent-bit.service - Fluent Bit
     Loaded: loaded (/lib/systemd/system/fluent-bit.service; enabled; vendor preset: enabled)
     Active: active (running) since Tue 2024-12-24 14:39:50 +07; 41s ago
       Docs: https://docs.fluentbit.io/manual/
   Main PID: 3346067 (fluent-bit)
      Tasks: 5 (limit: 6925)
     Memory: 8.8M
        CPU: 108ms
     CGroup: /system.slice/fluent-bit.service
             └─3346067 /opt/fluent-bit/bin/fluent-bit -c //etc/fluent-bit/fluent-bit.conf

Dec 24 14:39:50 Server fluent-bit[3346067]: [2024/12/24 14:39:50] [ info] [simd    ] disabled
Dec 24 14:39:50 Server fluent-bit[3346067]: [2024/12/24 14:39:50] [ info] [cmetrics] version=0.9.9
Dec 24 14:39:50 Server fluent-bit[3346067]: [2024/12/24 14:39:50] [ info] [ctraces ] version=0.5.7
Dec 24 14:39:50 Server fluent-bit[3346067]: [2024/12/24 14:39:50] [ info] [input:tail:tail.0] initializing
Dec 24 14:39:50 Server fluent-bit[3346067]: [2024/12/24 14:39:50] [ info] [input:tail:tail.0] storage_strategy='memory' (memory only)
Dec 24 14:39:50 Server fluent-bit[3346067]: [2024/12/24 14:39:50] [ info] [input:tail:tail.0] db: delete unmonitored stale inodes from the database: count=0
Dec 24 14:39:50 Server fluent-bit[3346067]: [2024/12/24 14:39:50] [ info] [sp] stream processor started
Dec 24 14:39:50 Server fluent-bit[3346067]: [2024/12/24 14:39:50] [ info] [output:es:es.0] worker #0 started
Dec 24 14:39:50 Server fluent-bit[3346067]: [2024/12/24 14:39:50] [ info] [output:es:es.0] worker #1 started
Dec 24 14:39:50 Server fluent-bit[3346067]: [2024/12/24 14:39:50] [ info] [input:tail:tail.0] inotify_fs_add(): inode=1051278 watch_fd=1 name=/var/log/axigen/webmail.mail3.longvan.net.txt
```

```
  GNU nano 6.2                                                /etc/fluent-bit/axigen_parser.conf
[PARSER]
  Name    axi.everything_parser
  Format  regex
# Default axigen install
  Regex   ^(?<logTime>\d{4}-\d{2}-\d{2} \d{2}:\d{2}:\d{2} \+\d{4}) (?<logLevel>[^ ]*) (?<host>[^ ]*) (?<service>[^:]*):(?<jobID>[^ :]*): (?<log>.*)$
  Time_Format %Y-%m-%d %H:%M:%S %z
# Axigen with AXI_LOG_TIMESTAMP_PRECISION enabled
# Regex   ^(?<logTime>\d{4}-\d{2}-\d{2} \d{2}:\d{2}:\d{2}.\d+ \+\d{4}) (?<logLevel>[^ ]*) (?<host>[^ ]*) (?<service>[^:]*):(?<jobID>[^ :]*): (?<log>.*)$
# Time_Format %Y-%m-%d %H:%M:%S.%L %z
  Time_Key  logTime
# Uncoment the below line to also include the logTime field that is used as a source for @timestamp
# Time_Keep On

[PARSER]
  Name    axi.security_parser
  Format  regex
# Default axigen install
  Regex   ^(?<logTime>\d{4}-\d{2}-\d{2} \d{2}:\d{2}:\d{2} \+\d{4}) (?<logLevel>[^ ]*) [^ ]* SECURITY:(?<service>[^;]*);(?<jobID>[^;]*);(?<remoteIP>[^;]*);(?<remotePort>[^;]*);(?<result>[^
  Time_Format %Y-%m-%d %H:%M:%S %z
# Axigen with AXI_LOG_TIMESTAMP_PRECISION enabled
# Regex   ^(?<logTime>\d{4}-\d{2}-\d{2} \d{2}:\d{2}:\d{2}\.\d+ \+\d{4}) (?<logLevel>[^ ]*) [^ ]* SECURITY:(?<service>[^;]*);(?<jobID>[^;]*);(?<remoteIP>[^;]*);(?<remotePort>[^;]*);(?<resu
# Time_Format %Y-%m-%d %H:%M:%S.%L %z
  Time_Key  logTime
# Uncoment the below line to include also logTime filed that is used as source for @timestamp
# Time_Keep On

[PARSER]
  Name    axi.webmail_parser
  Format  regex
  Regex   ^(?<logTime>\d{4}-\d{2}-\d{2} \d{2}:\d{2}:\d{2} \+\d{4}) (?<logLevel>[^ ]*) (?<host>[^ ]*) (?<service>[^:]*):(?<jobID>[^ :]*): (?<log>.*)$
  Time_Format %Y-%m-%d %H:%M:%S %z
  Time_Key  logTime
```

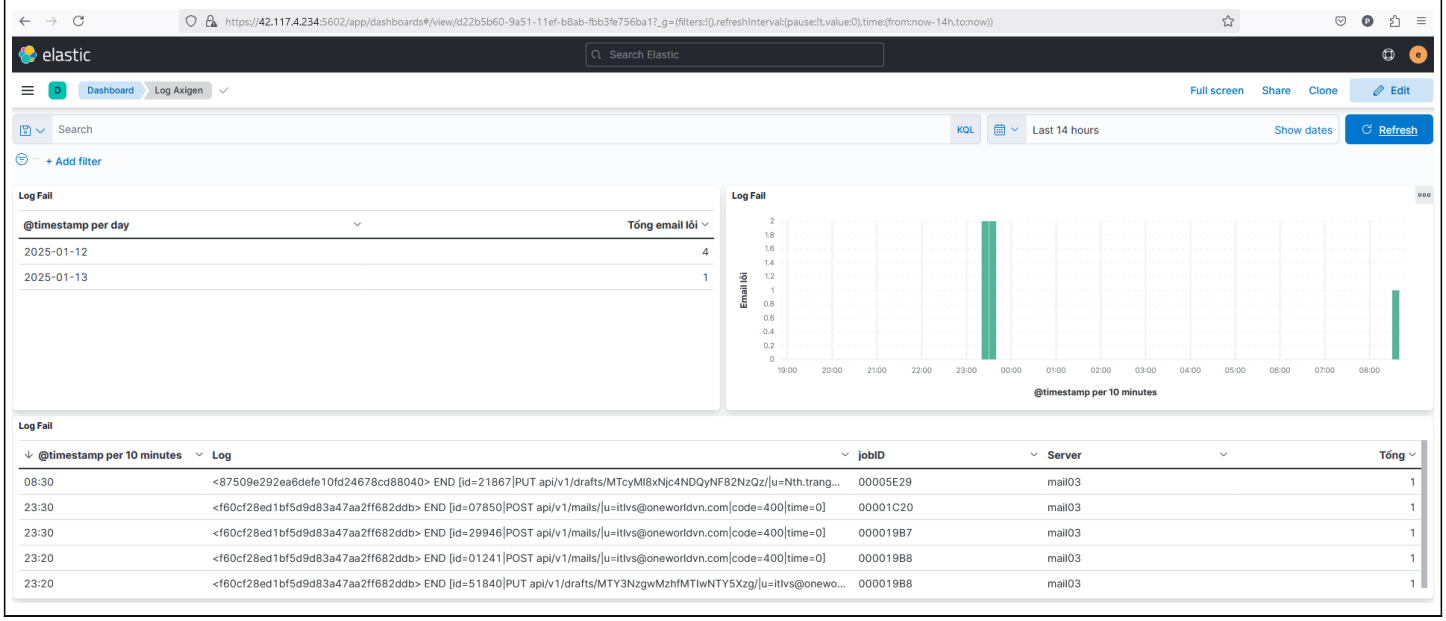
Đã setup xong fluent bit log nhưng đang bị lỗi cấu trúc log do phần server log trung gian đang thêm phần timetamp hostname ở mỗi dòng đầu tiên của log đang tìm cách xử lý

Link dashboard log mail lỗi
https://42.117.4.234:5602/app/dashboards#/view/d22b5b60-9a51-11ef-b8ab-fbb3fe756ba1?_g=(filters:!(),refreshInterval:(pause:!t,value:0),time:(from:now-14m,to:now))
user: admin

pass: Fy559kL4KkbJ



Bổ sung thêm phần log mail lỗi code 400



Lược sử

#1 - 24-12-2024 14:41 - Minh Pham

- Tập tin clipboard-202412241440-0kcul.png được thêm

- Mô tả cập nhật

#2 - 24-12-2024 14:42 - Minh Pham

- Tập tin clipboard-202412241442-nteis.png được thêm

- Mô tả cập nhật

#3 - 30-12-2024 10:05 - Minh Pham

- Mô tả cập nhật

#4 - 30-12-2024 10:05 - Minh Pham

- Mô tả cập nhật

#5 - 06-01-2025 09:15 - Minh Pham

- Tập tin clipboard-202501060914-26cf7.png được thêm

- Mô tả cập nhật

#6 - 06-01-2025 09:15 - Minh Pham

- Hết hạn thay đổi từ 30-12-2024 tới 07-01-2025

- Bát đầu thay đổi từ 23-12-2024 tới 30-12-2024

#7 - 13-01-2025 08:53 - Minh Pham

- Tập tin clipboard-202501130853-9a12t.png được thêm

- Mô tả cập nhật

#8 - 13-01-2025 08:53 - Minh Pham

- Trạng thái thay đổi từ In Progress tới Closed

Tập tin

clipboard-202412241440-0kcul.png	51,1 KB	24-12-2024	Minh Pham
clipboard-202412241442-nteis.png	54,2 KB	24-12-2024	Minh Pham
clipboard-202501060914-26cf7.png	108 KB	06-01-2025	Minh Pham
clipboard-202501130853-9a12t.png	127 KB	13-01-2025	Minh Pham