

## 31. GIẢI PHÁP-TESTING - Task #1375

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

### Filter log esxi trên logstash

09-12-2024 09:09 - Minh Pham

<b>Trạng thái:</b>	Closed	<b>Bắt đầu:</b>	08-12-2024
<b>Mức ưu tiên:</b>	Normal	<b>Hết hạn:</b>	22-12-2024
<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: Giảm dung lượng log trong 1 ngày trên elasticsearh

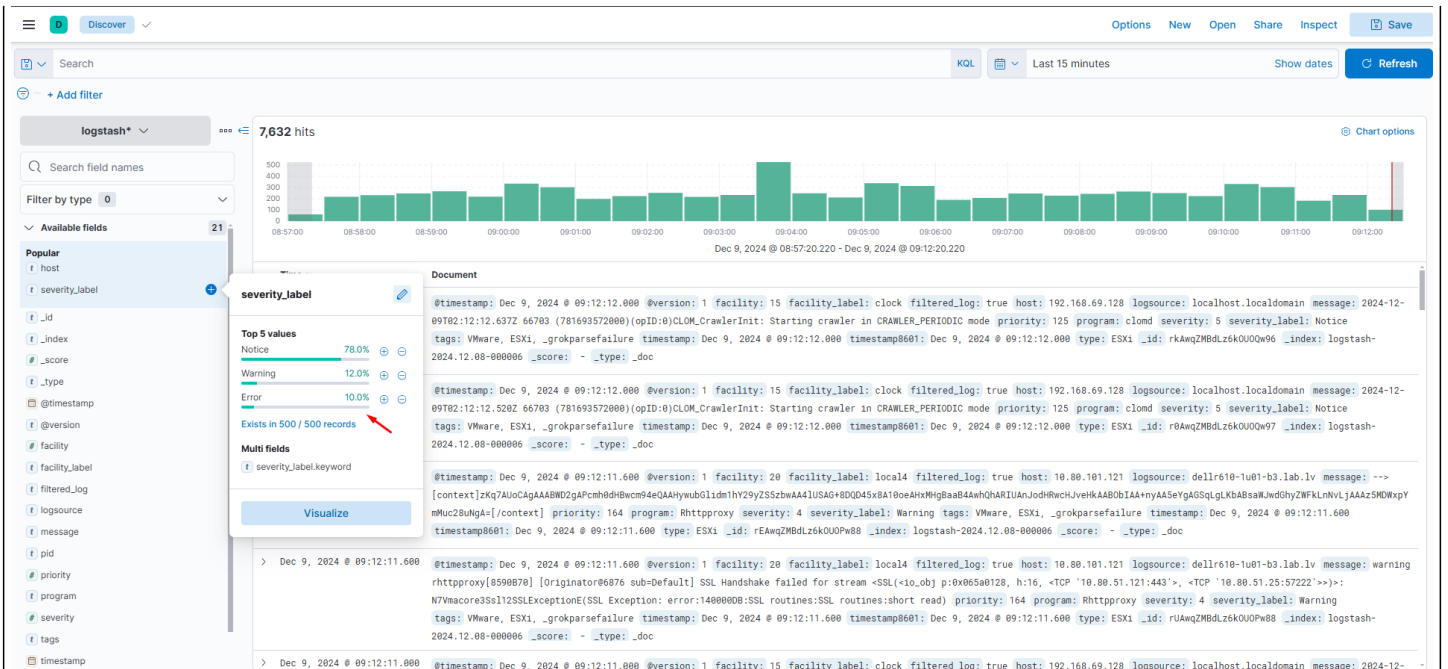
Kết quả thực hiện:

Filter lấy log esxi trên logstash

```
input {
  syslog {
    type => "ESXi"
    port => 514
    tags => ["VMware", "ESXi"]
    codec => plain
    {
      charset => "ISO-8859-1"
    }
  }
}
filter {
  # Parse log lines using grok pattern
  grok {
    match => {
      "message" => "%{TIMESTAMP_ISO8601:timestamp} %{LOGLEVEL:severity_label} %{DATA:component} %{GREEDYDATA:message}"
    }
  }

  # Filter for ERROR or WARN log levels
  if [severity_label] in ["Error", "Warning", "Notice"] {
    mutate {
      add_field => { "filtered_log" => "true" }
    }
  } else {
    drop {} # Drop logs that aren't ERROR or WARN
  }

  # Convert timestamp into @timestamp field for consistency
  date {
    match => ["timestamp", "ISO8601"]
  }
}
output {
  elasticsearch {
    hosts => "https://192.168.70.187:9200"
    cacert => '/etc/kibana/certs/ca/ca.crt'
    user => elastic
    password => lvsl23
    ssl_certificate_verification => false
    ssl => true
    # index => "esxi-logs-errors-warnings-%{+YYYY.MM.dd}"
  }
}
```



Giảm dung lượng log từ 2.2 Gb xuống còn khoảng 400 MB

## Index Management

[Index Management docs](#)

[Indices](#) | [Data Streams](#) | [Index Templates](#) | [Component Templates](#)

Update your Elasticsearch indices individually or in bulk. [Learn more.](#)

Include rollover indices  Include hidden indices

Name	Health	Status	Primaries	Replicas	Docs count	Storage size	Data stream
logstash-2024.12.08-000006	green	open	1	1	599321	172.9mb	
logstash-2024.12.04-000002	green	open	1	1	6712252	2.2gb	
logstash-2024.11.20-000001	green	open	1	1	33454758	11.1gb	
logstash-2024.12.07-000005	green	open	1	1	730005	215.3mb	
logstash-2024.12.05-000003	green	open	1	1	1137458	374.9mb	
logstash-2024.12.06-000004	green	open	1	1	747925	222.7mb	

### Lược sử

#### #1 - 09-12-2024 09:14 - Minh Pham

- Tập tin clipboard-202412090911-asqzp.png được thêm
- Tập tin clipboard-202412090912-tfe1v.png được thêm
- Tập tin clipboard-202412090913-7bqvc.png được thêm
- Mô tả cập nhật

#### #2 - 23-12-2024 09:40 - Minh Pham

- Trạng thái thay đổi từ In Progress tới Closed

### Tập tin

Tên tập tin	Kích thước	Ngày	Người tải lên
clipboard-202412090911-asqzp.png	35,3 KB	09-12-2024	Minh Pham
clipboard-202412090912-tfe1v.png	281 KB	09-12-2024	Minh Pham
clipboard-202412090913-7bqvc.png	84,4 KB	09-12-2024	Minh Pham