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

Trạng thái:	Closed	**Bắt đầu:**	08-12-2024
Mức ưu tiên:	Normal	**Hết hạn:**	22-12-2024
Phân công cho:	Minh Pham	**Tiến độ:**	0%
Chủ đề:		**Thời gian ước lượng:**	0:00 giờ
Phiên bản:		**Thời gian:**	0:00 giờ

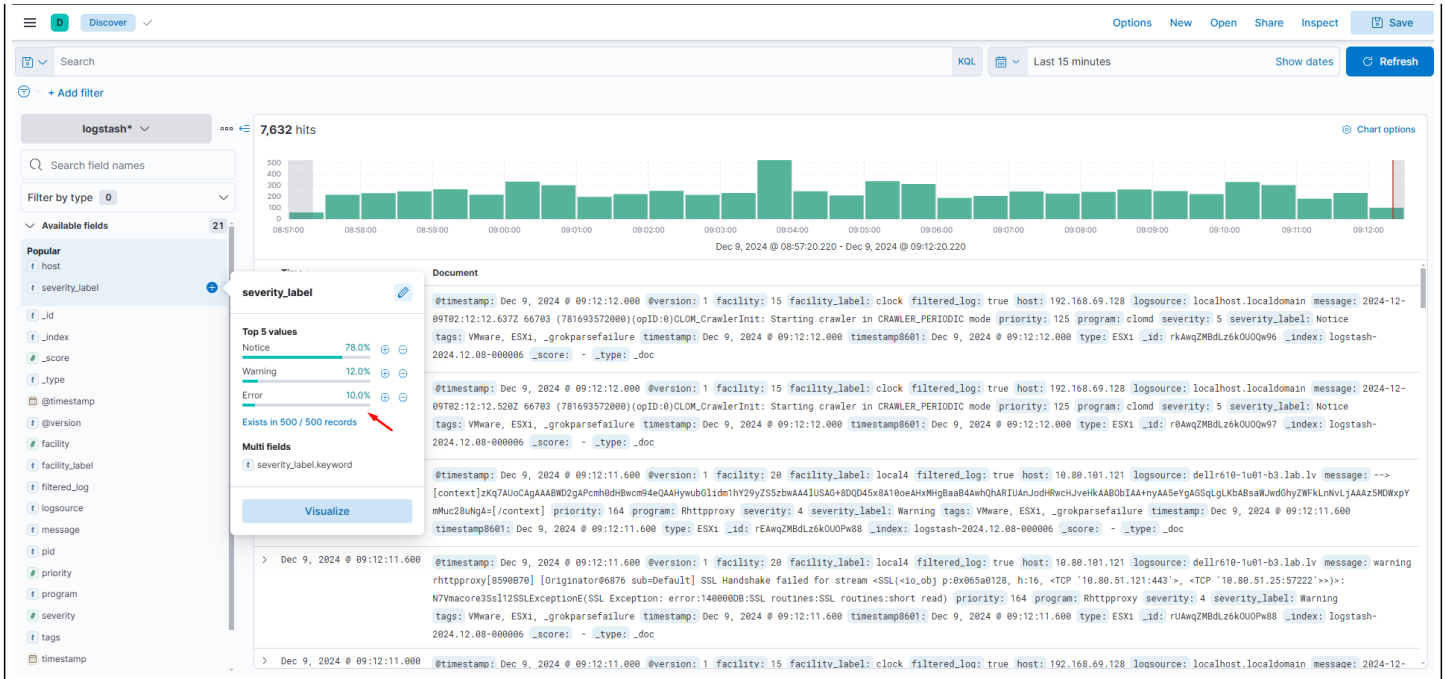
Mô tả

Mục tiêu: Giảm dung lượng log trong 1 ngày trên elasticseacrh

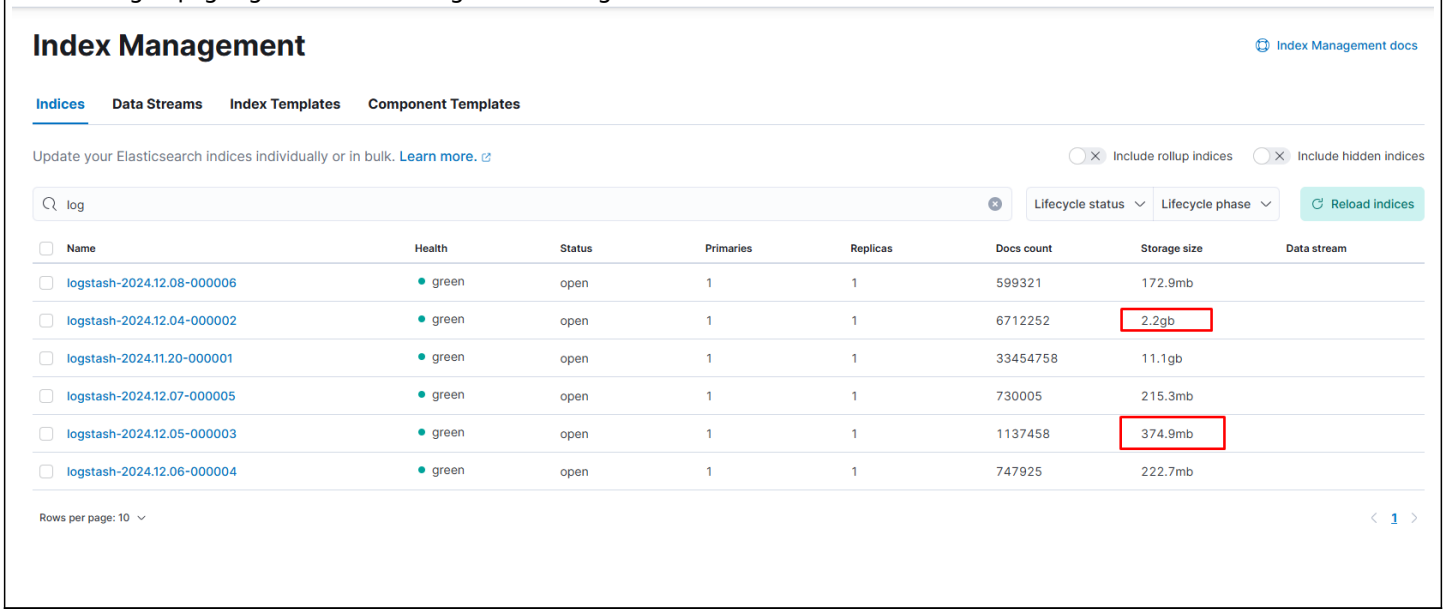
Kết quả thực hiện:

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 => lvs123
        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



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

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