# 1. Nội dung và hướng dẫn bài thực hành

## 1.1. Mục đích

Giúp sinh viên hiểu biết về công cụ Splunk - là một phần mềm chủ yếu được sử dụng để tìm kiếm, giám sát và kiểm tra dữ liệu do máy tạo ra thông qua giao diện web từ đó phân tích để đưa ra báo cáo cũng như cảnh báo với thời gian thực.

Đồng thời giúp sinh viên biết cách cài đặt và cấu hình Splunk, sử dụng công cụ Splunk để thu thập log và phân tích, giám sát hệ thống của mình.

## 1.2. Yêu cầu đối với sinh viên

* Có kiến thức cơ bản về hệ điều hành Linux, mô hình mạng khách/chủ.
* Có kiến thức về các loại log trong hệ điều hành, web.

## 1.3. Nội dung bài thực hành

* Tải bài lab:

imodule[**https://github.com/khuyennguyen128/AnNinhMang/releases/download/new/imodule.tar**](https://github.com/khuyennguyen128/AnNinhMang/releases/download/new/imodule.tar)

* **Khởi động bài lab:** 
  + Vào terminal, gõ:

*labtainer -r ptit-splunk-n13*

*(chú ý: sinh viên sử dụng email stu.ptit.edu.vn của mình để nhập thông tin email người thực hiện bài lab khi có yêu cầu, để sử dụng khi chấm điểm)*

Sau khi khởi độg xong 3 terminal ảo sẽ xuất hiện, một cái đại diện cho máy splunk, máy client và máy server. Biết rằng 3 máy nằm cùng mạng LAN.

* Trên terminal **client** sử dụng lệnh sau để truy cập vào web Splunk:

*firefox http://172.10.0.10:8000*

* Trên terminal **server** sẽ thực hiện các thao tác để Splunk thu thập log.
* **Kết thúc bài lab:**
  + Trên terminal đầu tiên sử dụng câu lệnh sau:

*stoplab ptit-splunk-n13*

* + Khi bài lab kết thúc, một tệp zip lưu kết quả được tạo vào một vị trí được hiển thị bên dưới stoplab.
* **Khởi động lại bài lab:**
  + Trong quá trình làm bài sinh viên cần thực hiện lại bài lab, dùng câu lệnh:

*startlab -r ptit-splunk-n13*

* + - Cài đặt và cấu hình Splunk trong container Splunk:
* Tải và cài đặt Splunk Index
* Cấu hình Splunk để lắng nghe trên cổng cụ thể (ví dụ: cổng 9997) để nhận log từ container "logserver".
* Đảm bảo rằng Splunk được cấu hình để lưu trữ dữ liệu log.
* Cấu hình máy tạo log (container "logserver"):
* Tải và cài đặt Splunk Forwarder để chuyển tiếp log đến splunk
* Cài đặt các thư viện và ứng dụng cần thiết để tạo và gửi log
* Cấu hình máy tạo log để gửi log đến Splunk container qua giao thức đã mô tả.
* Truy cập và xem dữ liệu log từ container "clientntk":
* Truy cập giao diện web của Splunk từ container "clientntk" thông qua trình duyệt web.
* Tìm kiếm, xem, và tạo các truy vấn trên dữ liệu log đã được ghi vào Splunk từ container "logserver".
  + - Các nhiệm vụ cần phải thực hiện để thực hành thành công:

***Nhiệm vụ 1: Cài đặt và cấu hình máy chủ log và máy chủ Splunk***

* Sinh viên cần cấu hình Splunk trên máy splunkanm và cấu hình Splunk Forwarder trên máy logserver để hai bên giao tiếp được log với nhau.

***Nhiệm vụ 2: Tìm được địa chỉ IP của các máy và cổng đang mở:***

* Sinh viên cần thực hiện nmap để tìm ra địa chỉ IP của máy Splunk và cổng web đang mở.
* Đồng thời sử dụng lệnh ping để kiểm tra kết nối tới máy chủ web Splunk
* Khi đầy đủ thông tin trên sinh viên có thể truy cập vào web Splunk và thu được log của máy logserver

***Nhiệm vụ 3: Tạo index và kiểm tra xem log của logserver đã được chuyển tới máy chủ web Splunk hay chưa:***

* Sinh viên cần thực hiện một truy vấn trong giao diện Splunk để kiểm tra xem có log của logserver chưa.
* Cụ thể: sinh viên sẽ thu thập toàn bộ log của máy logserver trong thời gian đã cho trước

*Câu truy vấn: index = “logserver”*

***Nhiệm vụ 4: Tạo truy vấn và bắt sự kiện log xảy ra trên máy logserver:***

* Sinh viên cần thực hiện một truy vấn trong giao diện Splunk để tìm kiếm log của logserver.

***Nhiệm vụ 5: Tạo report từ dữ liệu log thu được:***

* Sinh viên cần tạo một báo cáo hoặc biểu đồ từ dữ liệu log bằng các tính năng của Splunk.
* Xác định xem báo cáo hoặc biểu đồ có được tạo ra một cách chính xác và thể hiện thông tin log một cách hợp lý hay không.

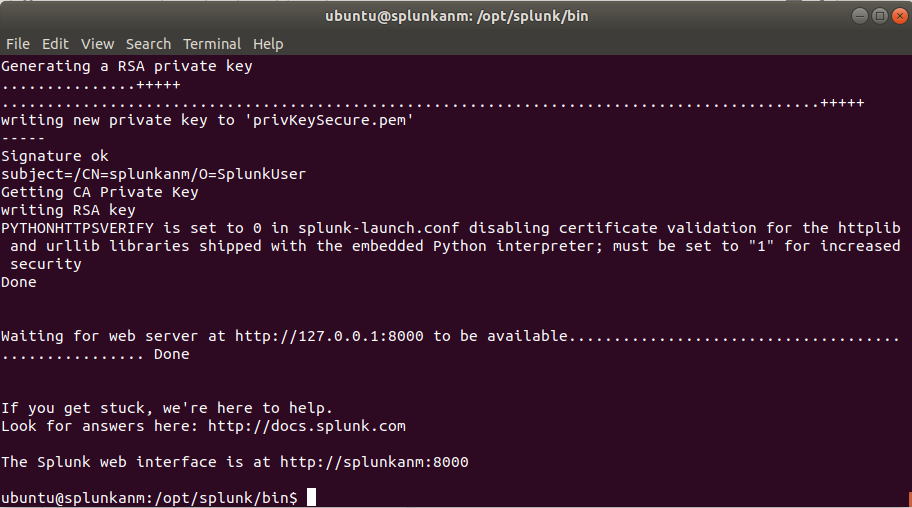
***Nhiệm vụ 6: Tạo dashboard từ dữ liệu log để trực quan hoá dữ liệu:***

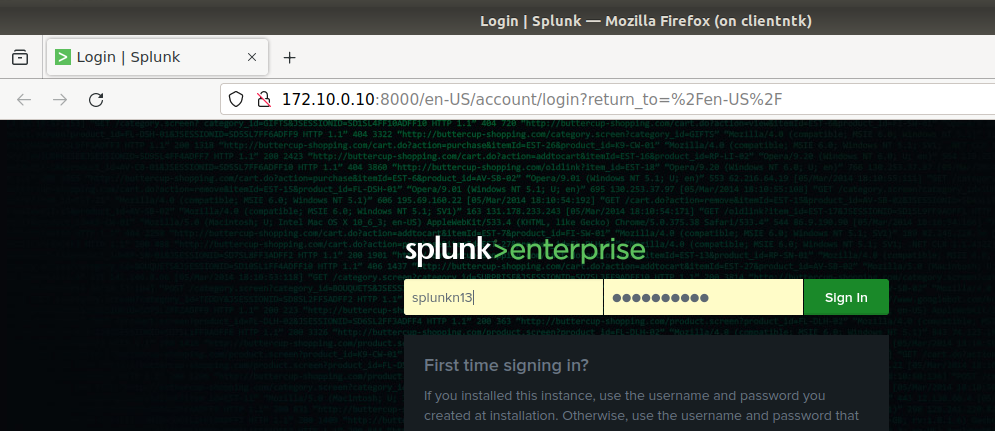
* Sinh viên cần tạo một báo cáo hoặc biểu đồ từ dữ liệu log bằng các tính năng của Splunk.
* Xác định xem báo cáo hoặc biểu đồ có được tạo ra một cách chính xác và thể hiện thông tin log một cách hợp lý hay không.

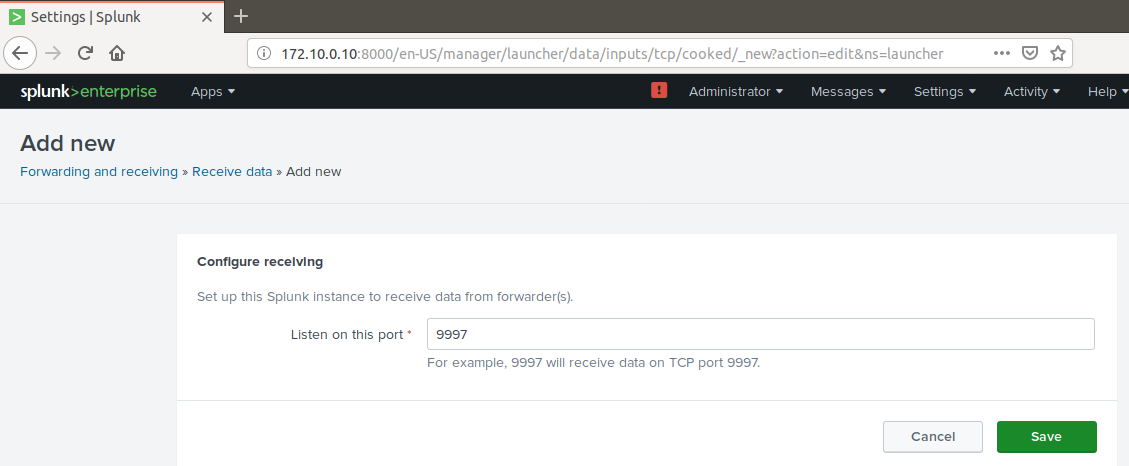
***Nhiệm vụ 7: Tạo alert cảnh báo về sự kiện đăng nhập quá số lần cho phép:***

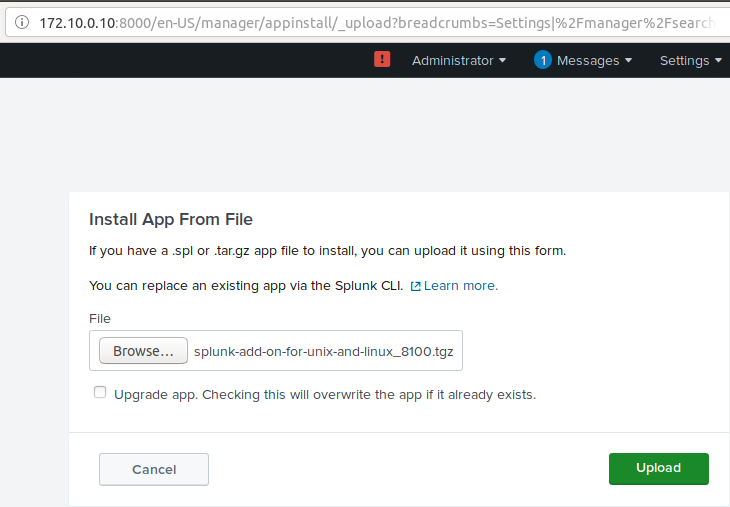
* Sinh viên cần tạo thành công một cảnh báo về sự kiện sử user trên logserver đăng nhập tài khoản quá số lần cho phép
* Sau đó alert này sẽ được gửi cảnh báo qua thông báo hoặc qua log event

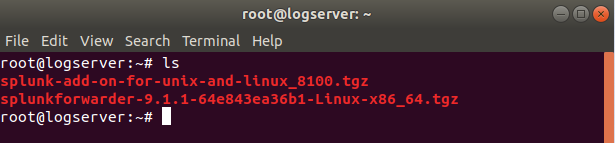
**Task 1: Cài đặt và cấu hình máy chủ log và máy chủ Splunk**

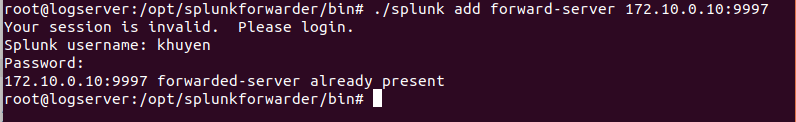


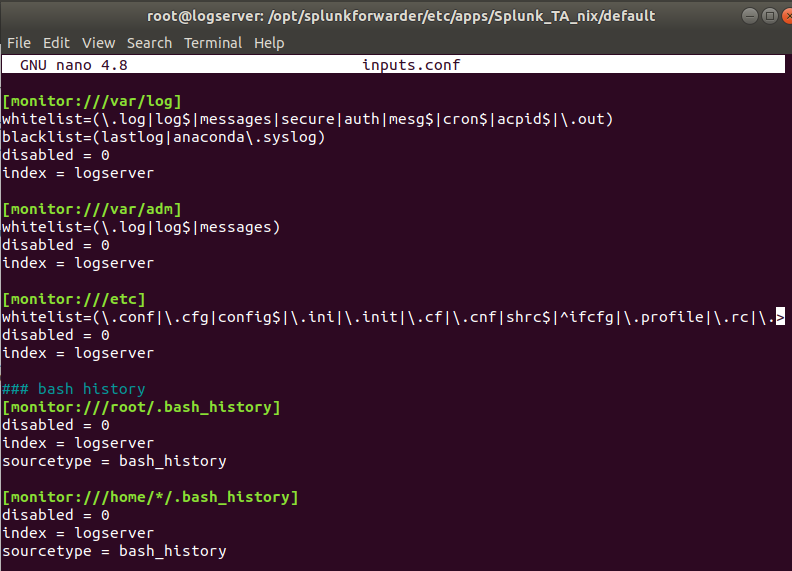




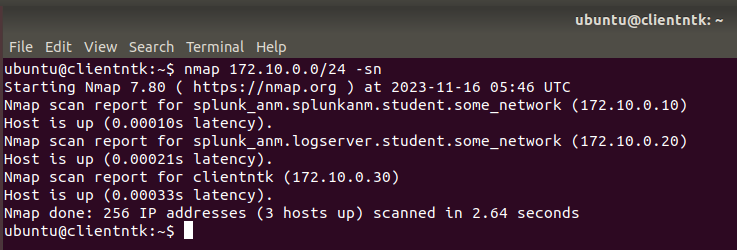


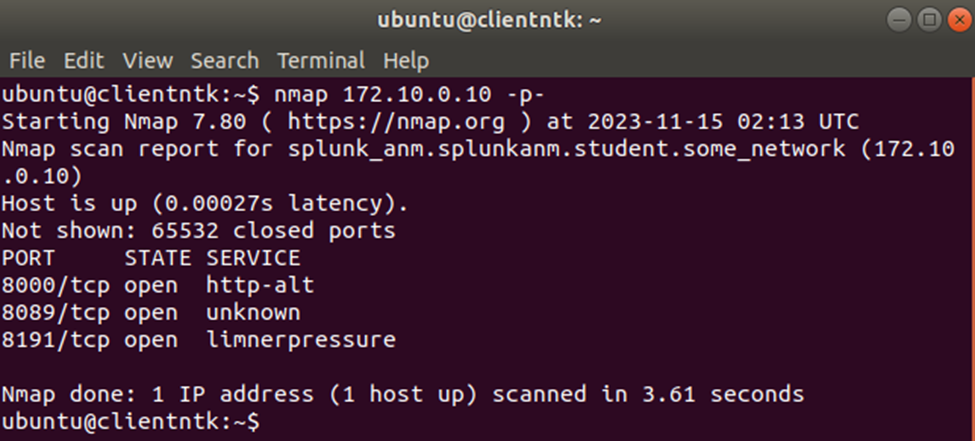


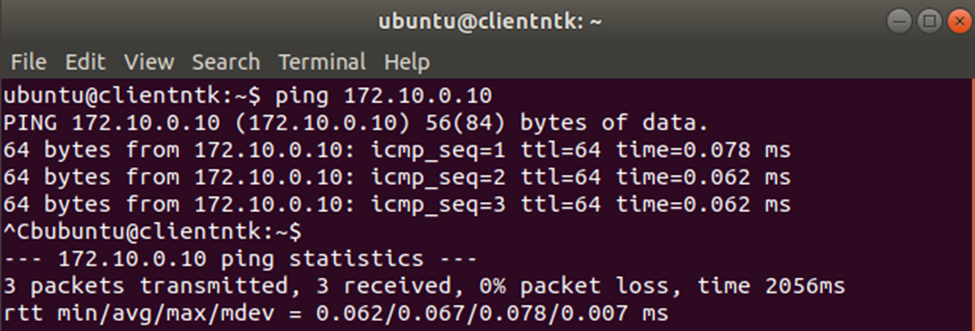




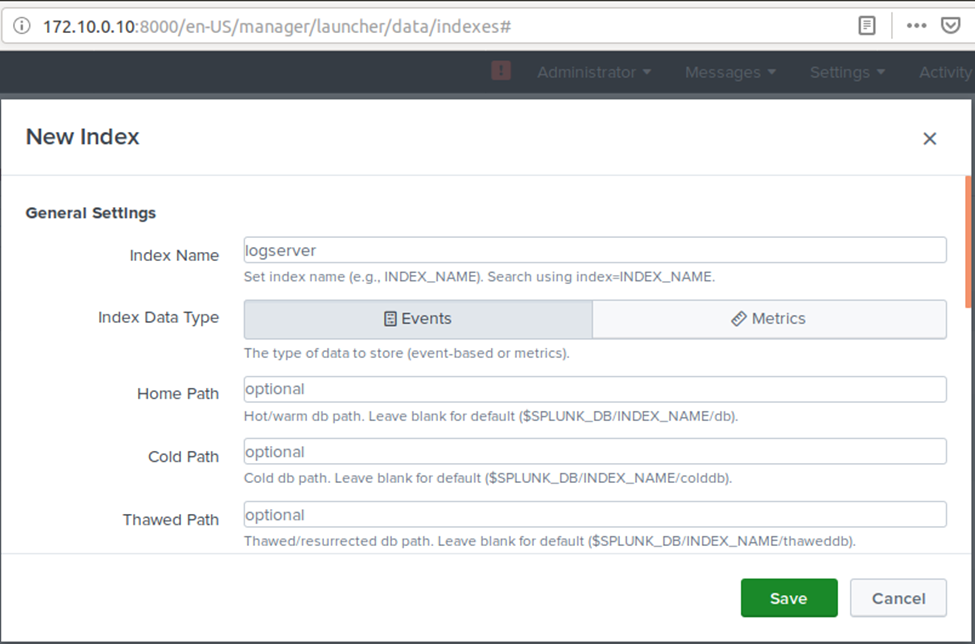
**Task 2: Tìm được địa chỉ IP của các máy và cổng đang mở**



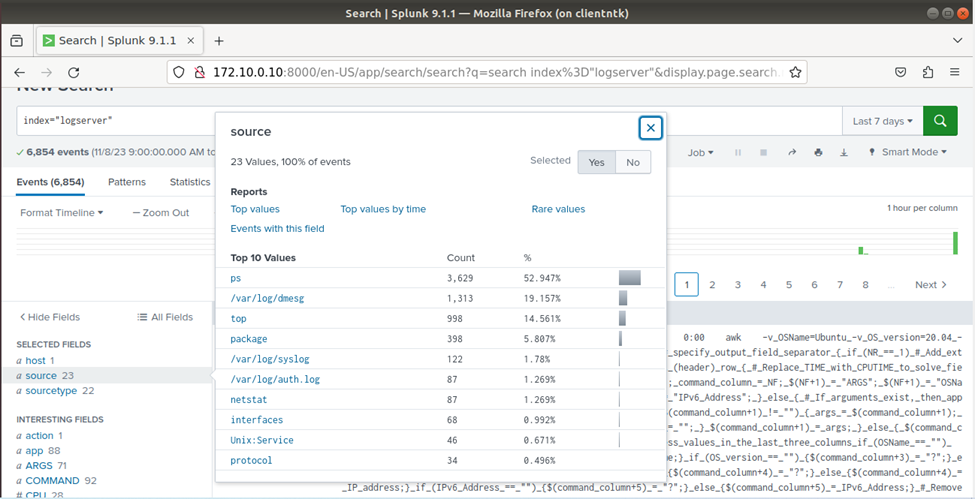


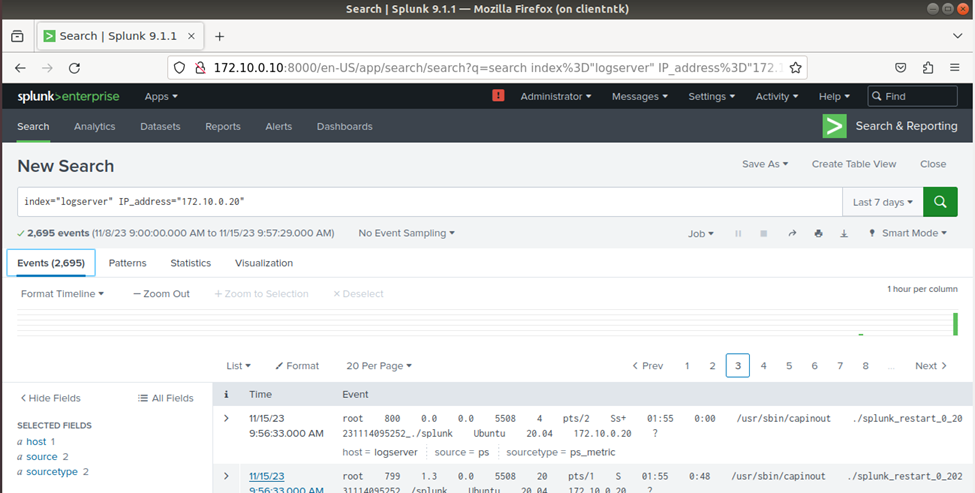


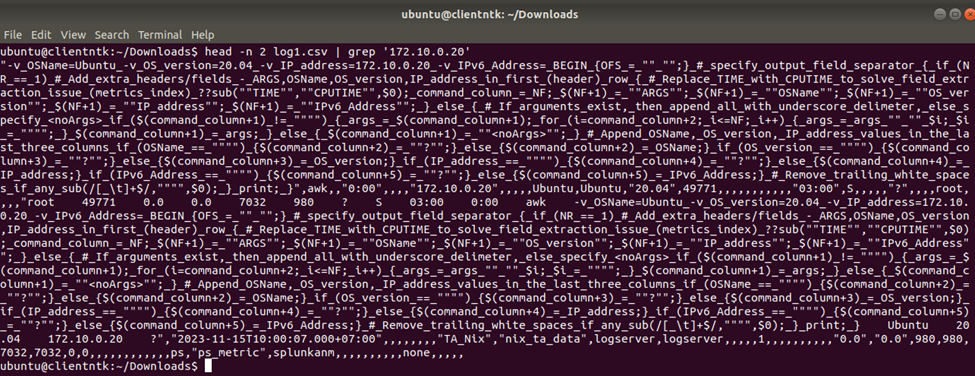
**Task 3: Tạo index và kiểm tra xem log của logserver đã được chuyển tới máy chủ web Splunk hay chưa:**



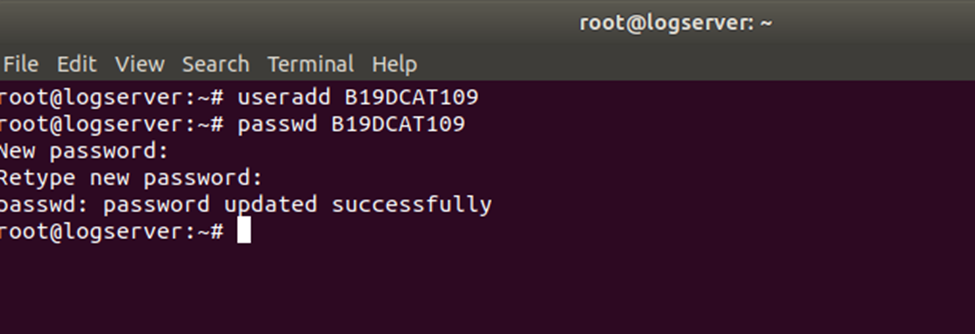
Hình 32. Tạo index để logserver sẽ đổ log về index này

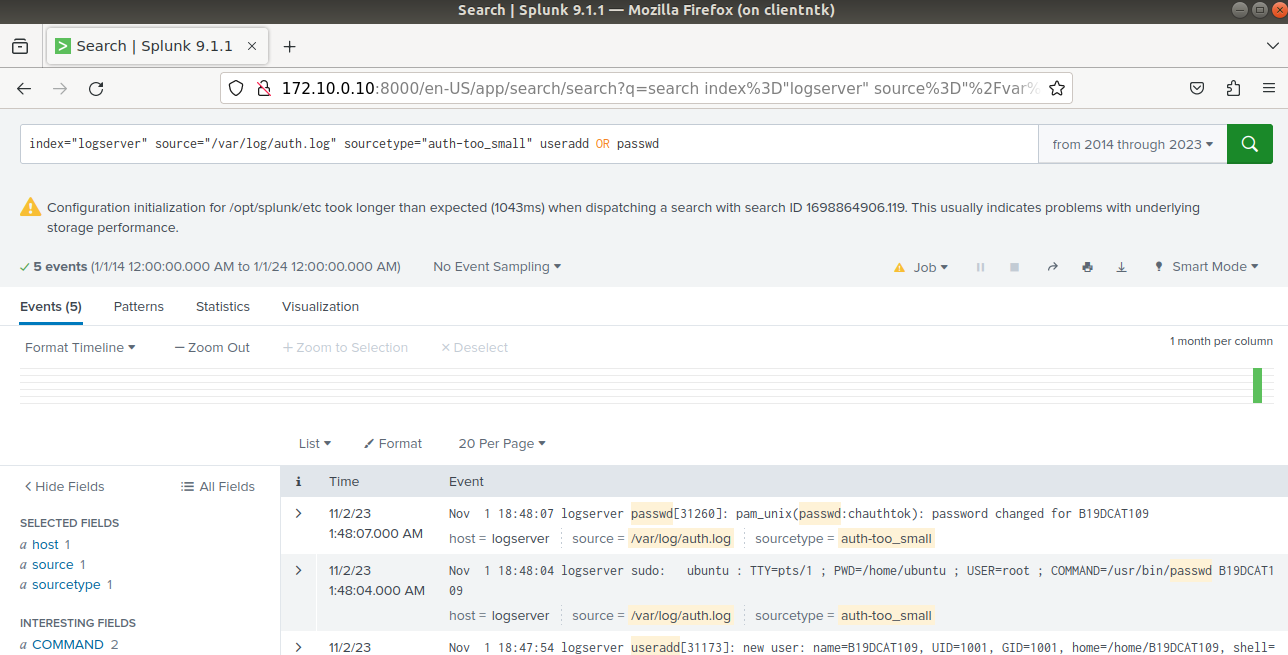


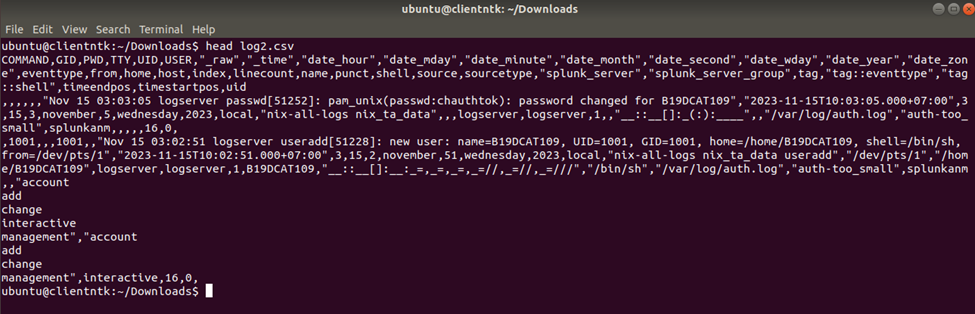




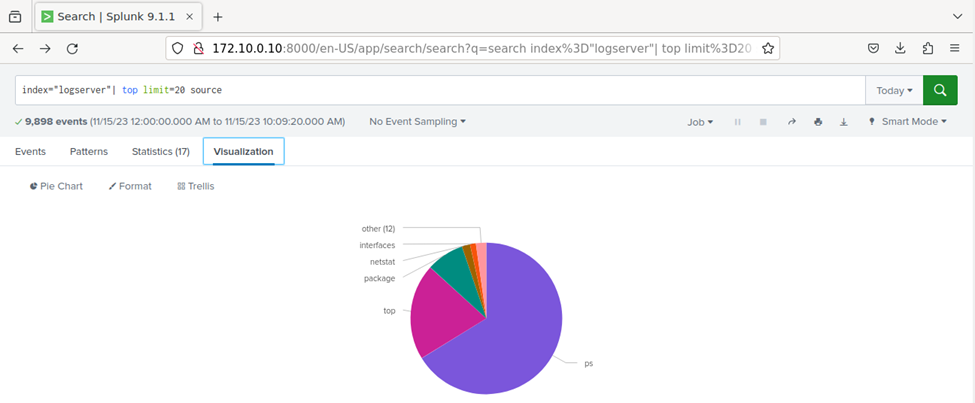
**Task 4: Truy vấn tìm kiếm dữ liệu log**

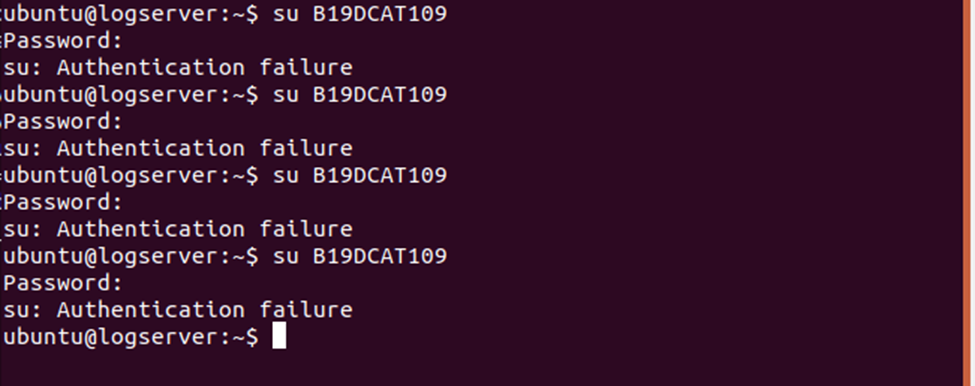


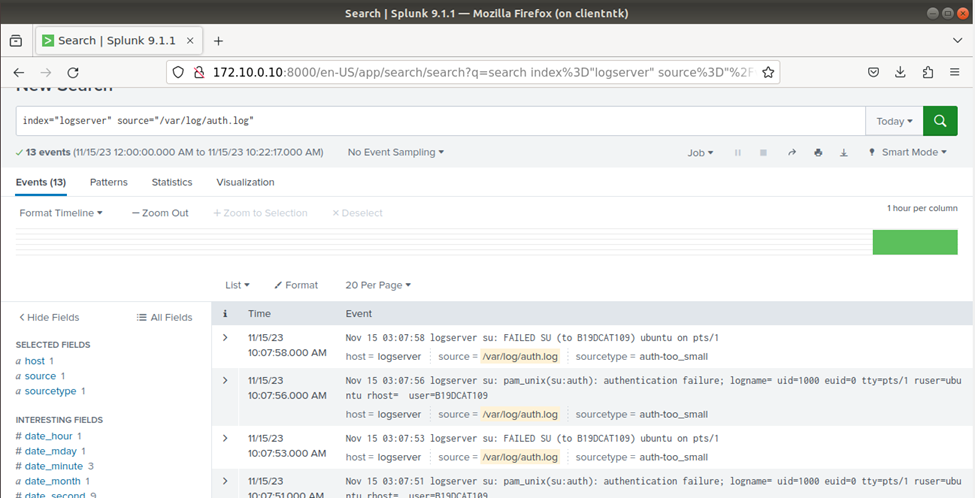


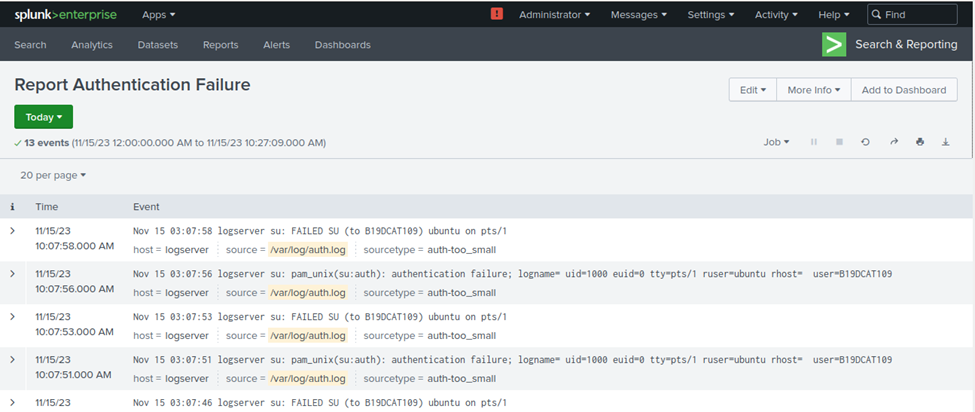


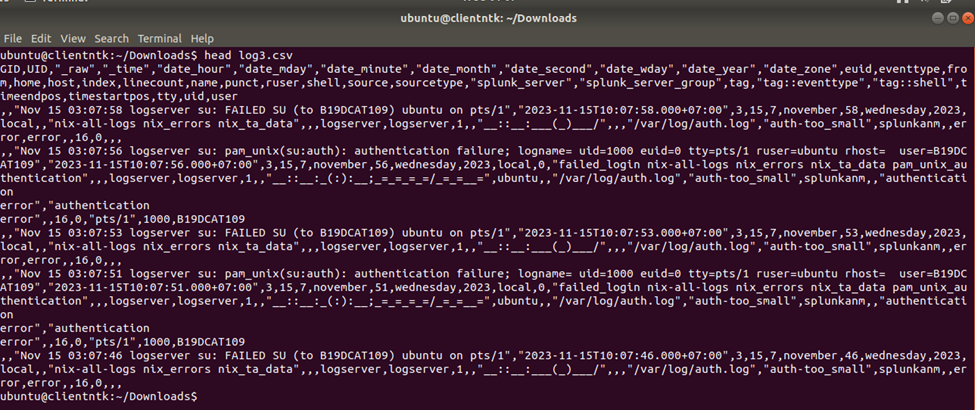
**Task 5: Tạo báo cáo( Reports) cho tìm kiếm định kỳ:**

****

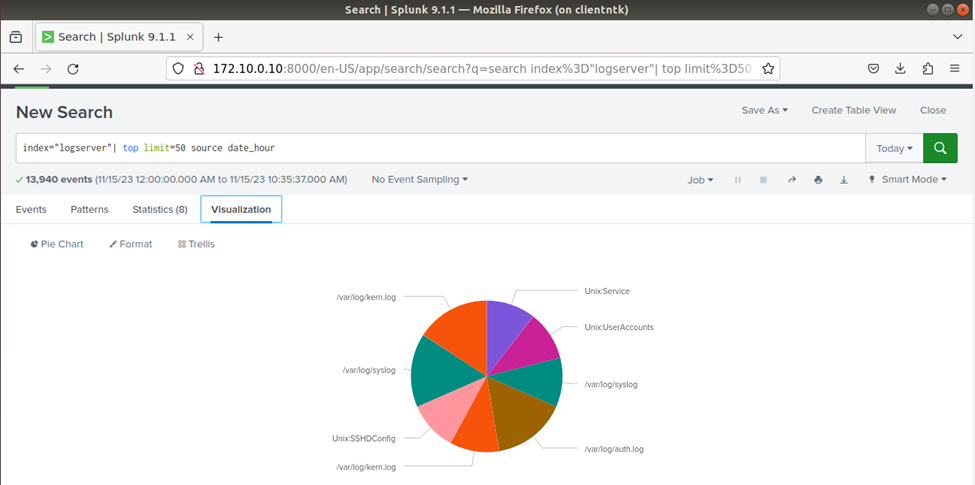


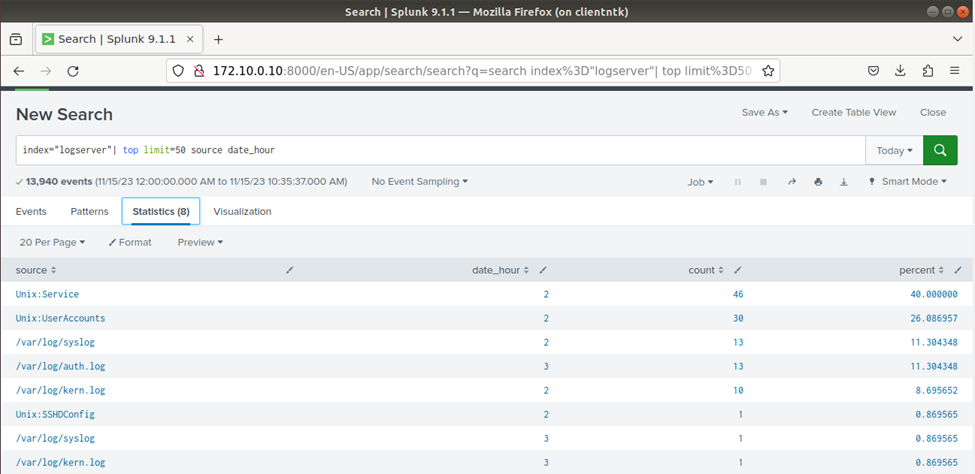


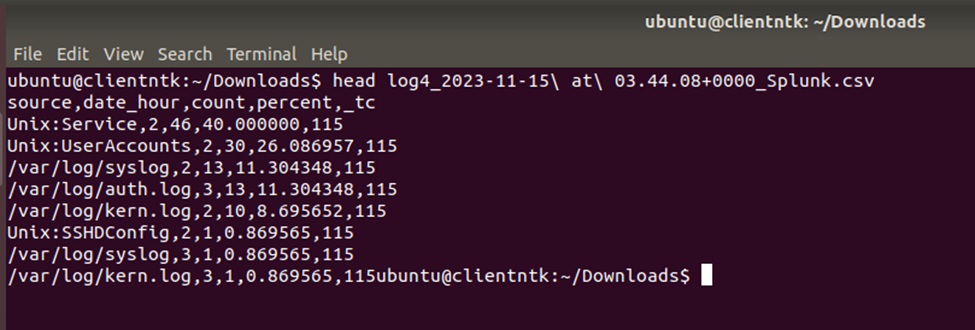




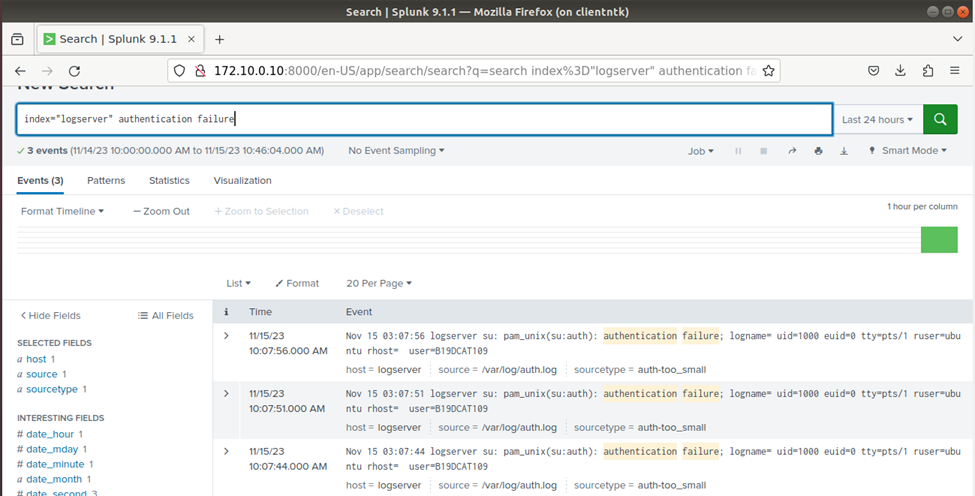
**Task 6: Tạo bảng điều khiển (DashBoards) để trực quan hoá dữ liệu.**

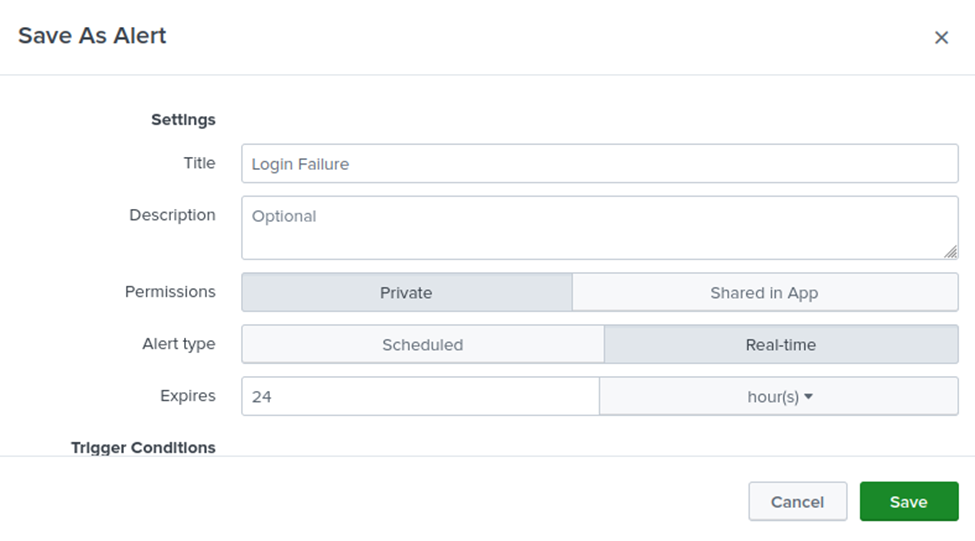


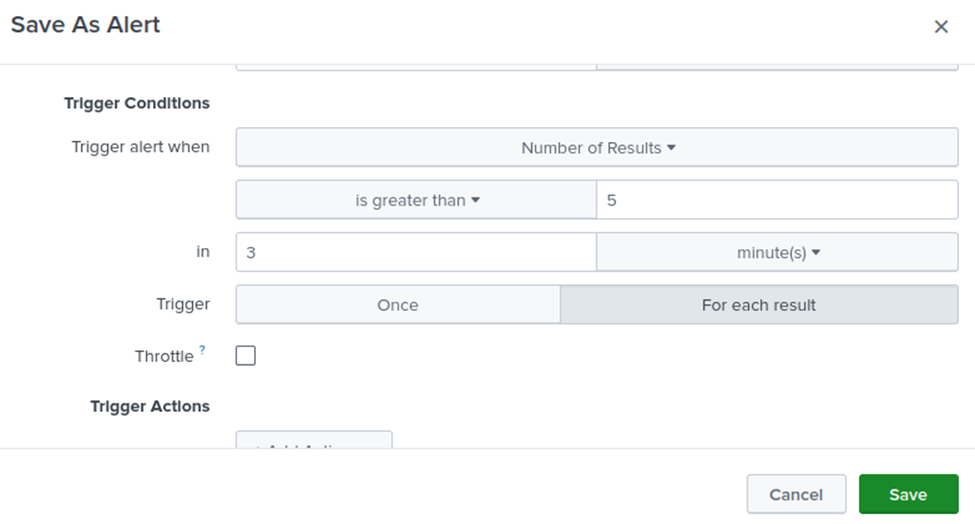


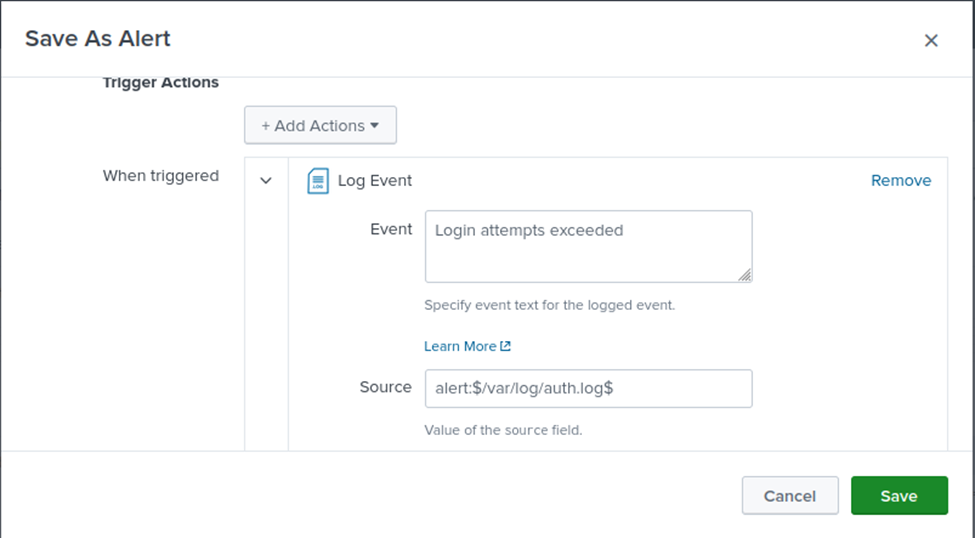


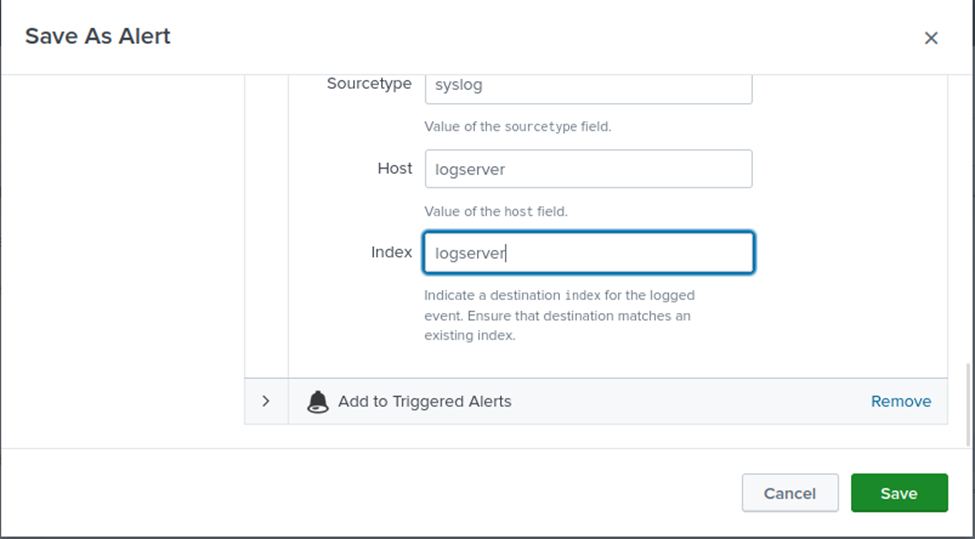
**Task 7: Tạo cảnh báo khi số lần đăng nhập của người dùng quá số lần cho phép**

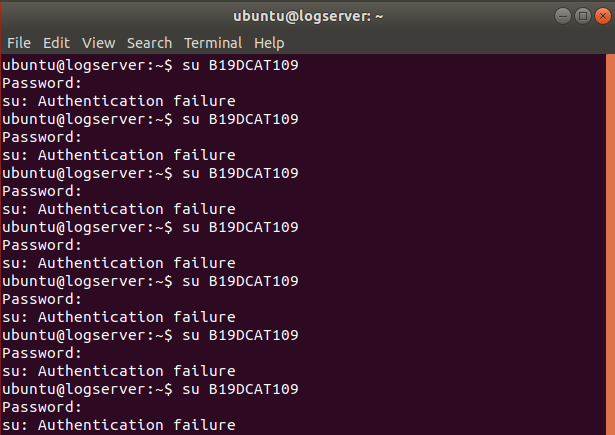


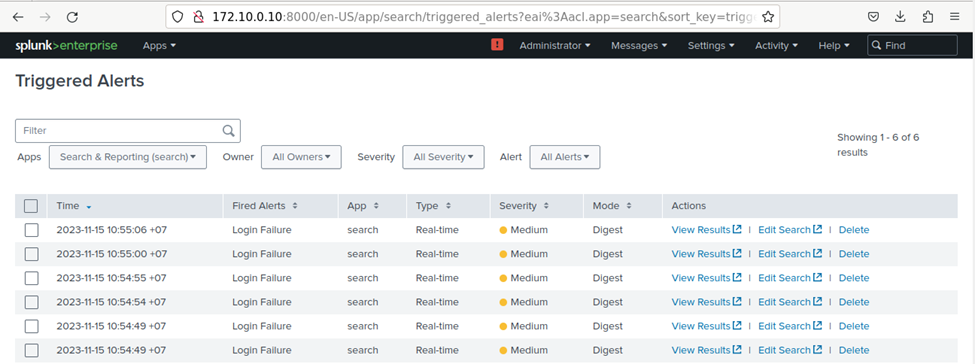


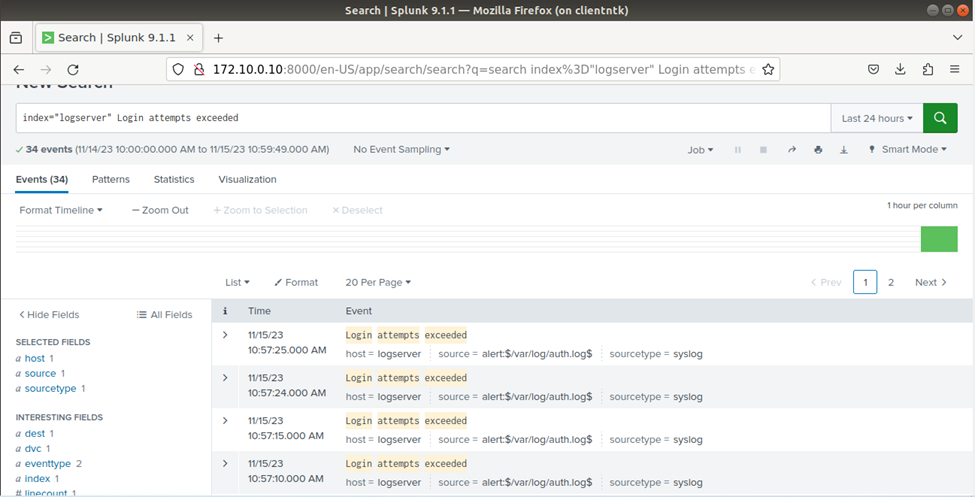


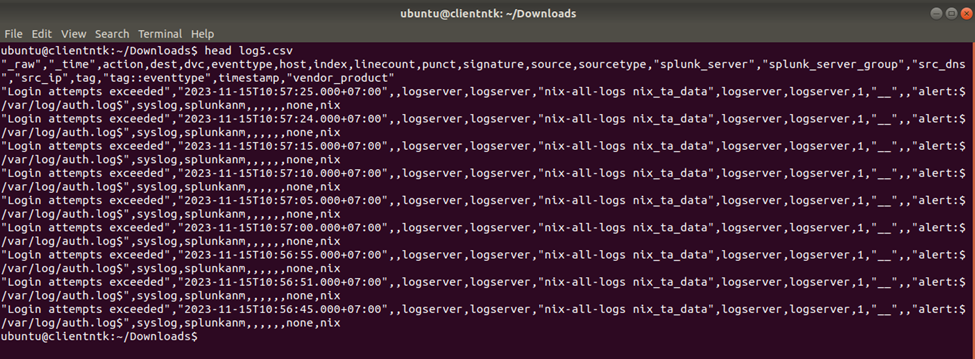


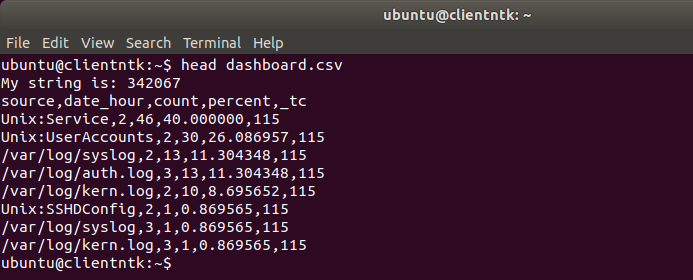










****