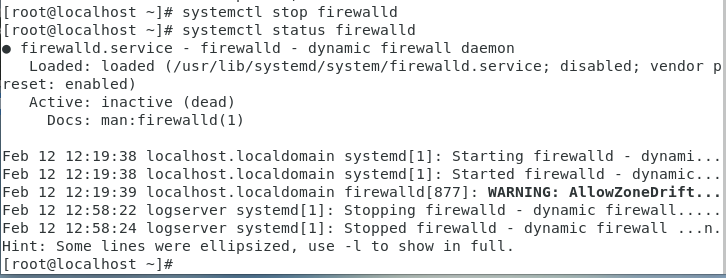
**I, Cấu hình input log từ syslog server vào splunk server (trên Linux)**

Chuẩn bị :

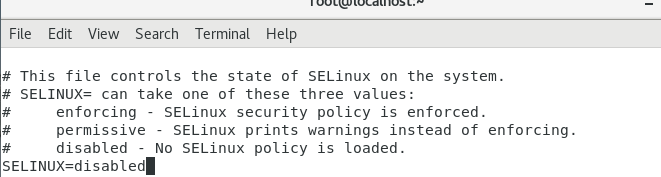
+1 máy centos hostname splunk.local , ip address 192.168.0.114 đóng vai trò là splunk server

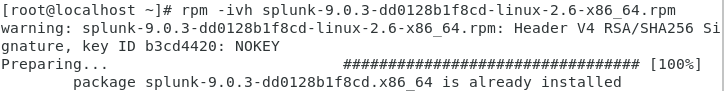
  
+1 máy centos client hostname là logserver, ip address 192.168.0.115 đóng vai trò là syslog server gửi log về cho splunk server.

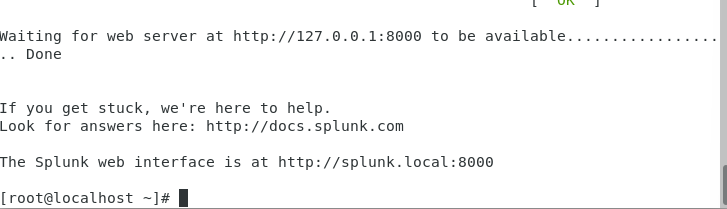
  
Tắt firewall, selinux trên cả 2 máy:  
+Tắt firewall : # systemctl stop firewalld

  
+Tắt Selinux: # vi /etc/sysconfig/selinux

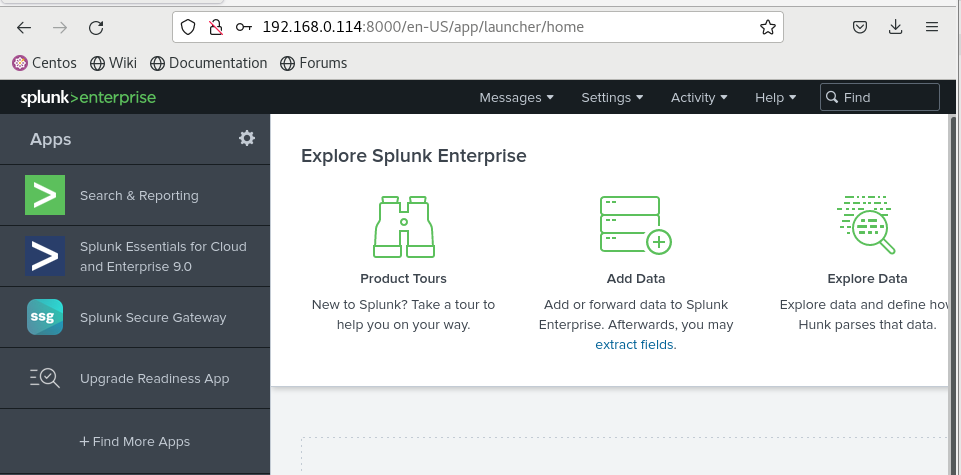
Sửa “SELINUX=enforcing” thành”SELINUX=disabled”

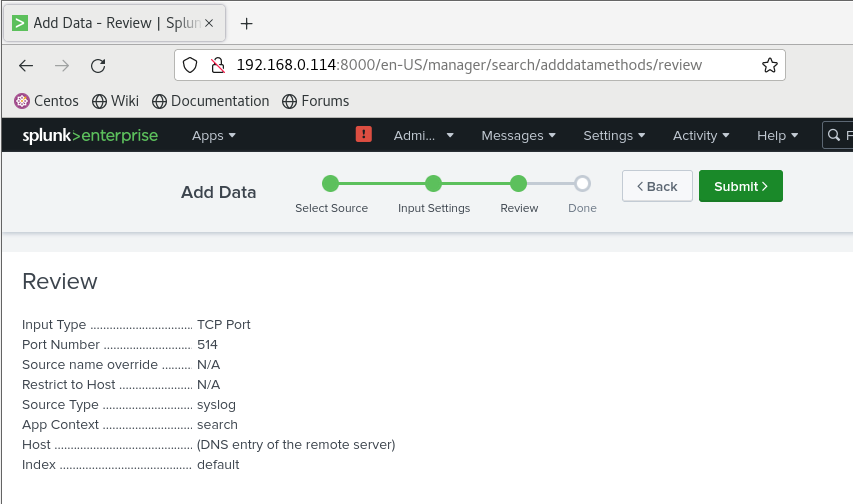


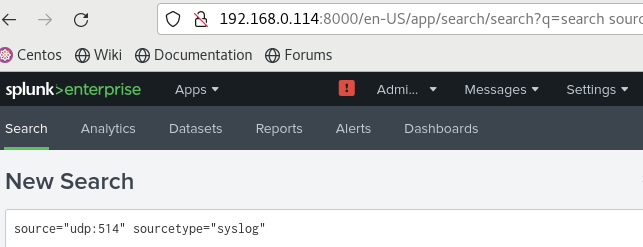
Trên máy Splunk server:  
Tải gói splunk rpm 64 bit từ trang web www.splunk.com và cài đặt dưới quyền admin  
  
Gõ đường dẫn để chạy splunk:  
# /opt/splunk/bin/splunk start  
Bảng license agreement hiện ra, chọn y để khởi động.

/opt  
Splunk đã được cài đặt thành công  
Để splunk khởi động mỗi khi restart máy gõ lệnh:  
# /opt/splunk/bin/splunk enable boot-start

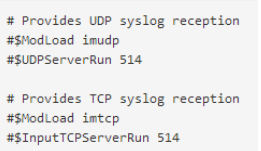
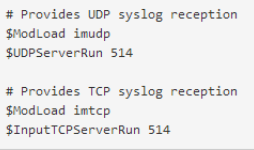
Vào giao diện web của splunk, chọn mở trình duyệt(firefox) rồi gõ đường dẫn 192.168.0.114:8000 để vào giao diện splunk web.

  
Sau khi truy cập vào giao diện web splunk, để nhận log từ syslog server , ta vào input data, chọn tcp, add  
port listen là 514 source type là syslog và có thể tùy chọn lắng nghe từ nhiều nguồn hoặc từ nguồn chỉ định(192.168.0.115).Sau đó save.

  
Vào input data nhấp chọn udp và làm tương tự như ở trên tcp

  
Hoàn tất quá trình cài đặt và cấu hình splunk.

Trên máy SyslogServer :  
Cài đặt syslog server  
# Yum install rsyslog  
Sau khi cài đặt xong, vào /etc/rsyslog.conf chỉnh sửa nội dung file rsyslog.conf để mở port 514 cho syslog(bỏ 2 dấu #)

Đồng thời thêm vào 2 dòng dưới section #####RULES#####  
\*.\* @192.168.0.114  
Mail.\* @192.168.0.114  
Sau đó thoát ra save file lại và restart rsyslog bằng lệnh :  
# service rsyslog restart  
Sau đó thử switch user trên syslog server để sản sinh log.Sau đó qua kiểm tra bên splunk server xem log đó đã được send qua hay chưa

