Splunk Lab Setup Documentation

# Lab Setup Overview

This document details the setup of a Splunk lab environment for security monitoring and threat detection.   
The architecture includes a Linux virtual machine with a Splunk Universal Forwarder and a Windows host running Splunk Enterprise. The environment is designed to simulate and detect common attack scenarios such as **brute-force attacks**, **lateral movement**, **log tampering**, and **user account creation**.

# Architecture

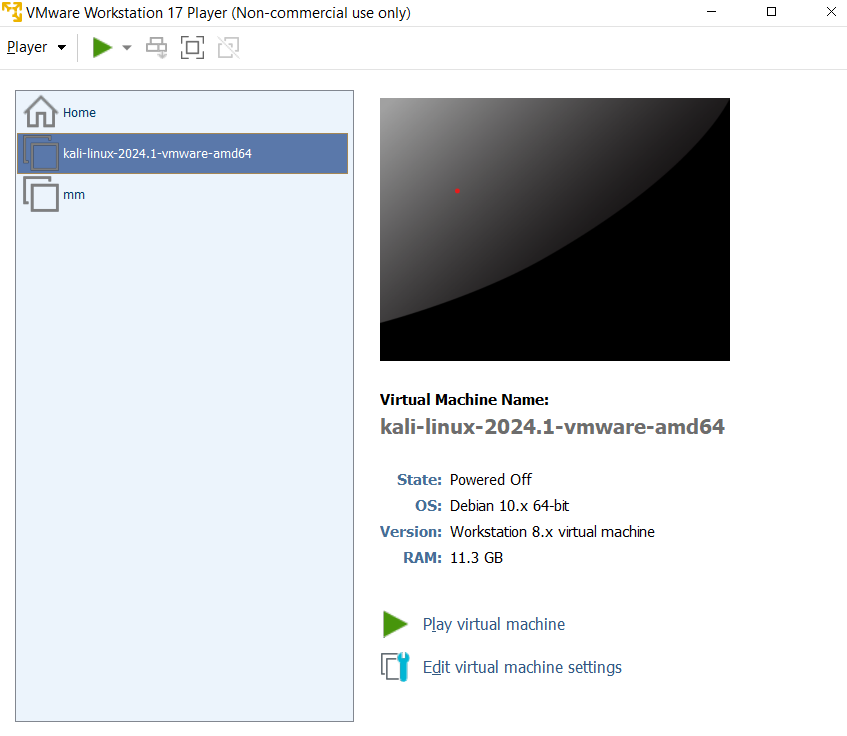
- **Windows Host Machine**:  
 - Operating System: Windows 10/11  
 - Software: Splunk Enterprise  
  
- **Linux Virtual Machine**:  
 - Operating System: Kali Linux/Ubuntu  
 - Software: Splunk Universal Forwarder  
  
- **Communication**: Linux VM forwards logs to Splunk Enterprise on Windows via TCP port 9997.

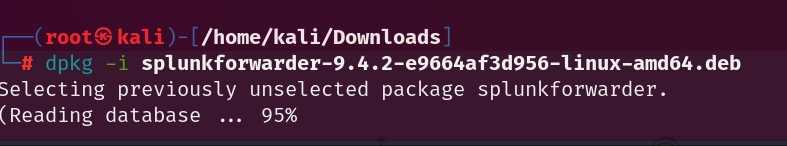
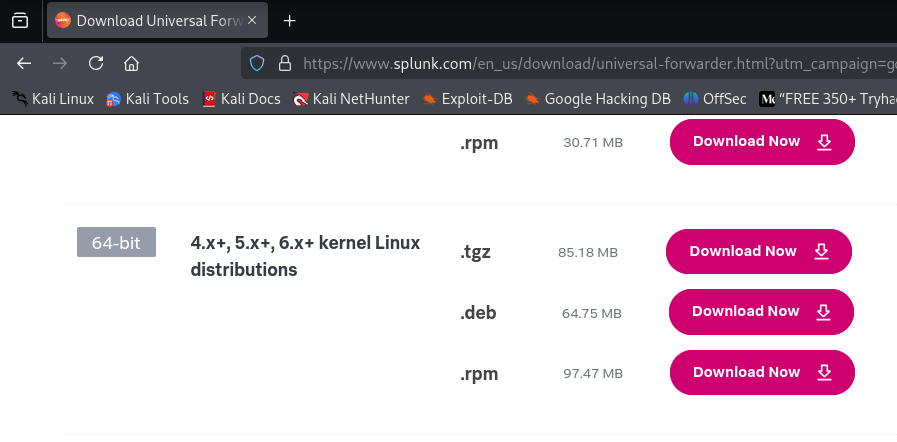
# Tools Used

- Splunk Enterprise  
- Splunk Universal Forwarder  
- Syslog (/var/log/syslog)  
- Auth logs (/var/log/auth.log) - Audit logs (/var/log/auditd/audit.log)  
- Custom attack simulation tools (ex : Hydra)

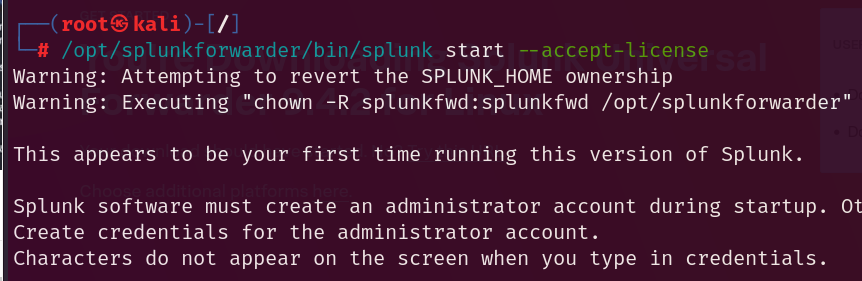
# Splunk Forwarder Configuration

1. Install Splunk Forwarder on Linux VM:

  
- Download and extract Splunk Forwarder , according to you machine type.



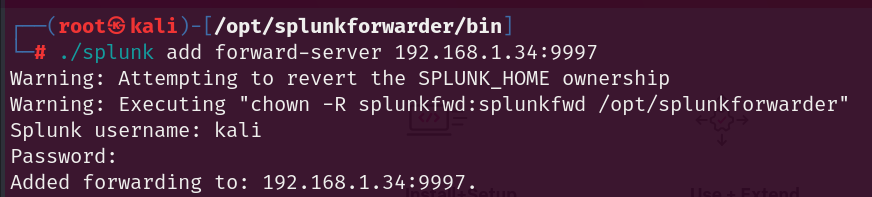
2. Start Splunk Forwarder:



sudo /opt/splunkforwarder/bin/splunk start --accept-license

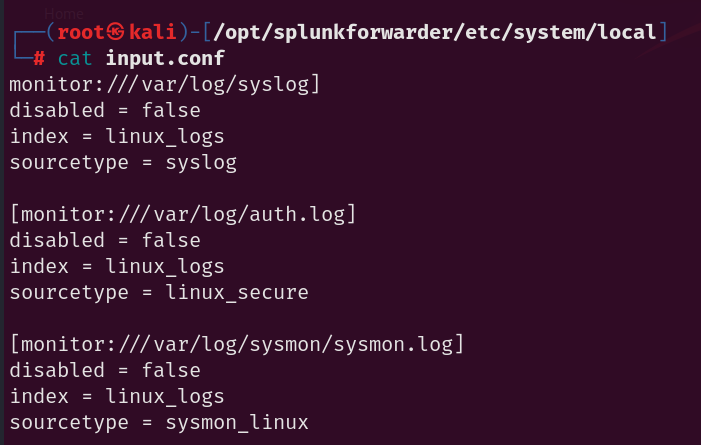
1. Configure Splunk Forward Server:

This will forward our defined logs in inputs.conf to splunk enterprise server hosted on windows machine.

  
sudo /opt/splunkforwarder/bin/splunk add forward-server <Windows\_IP>:9997

**Note** : This step , might be done again , if machine restarts with new IP\_address .

1. Monitor Logs:

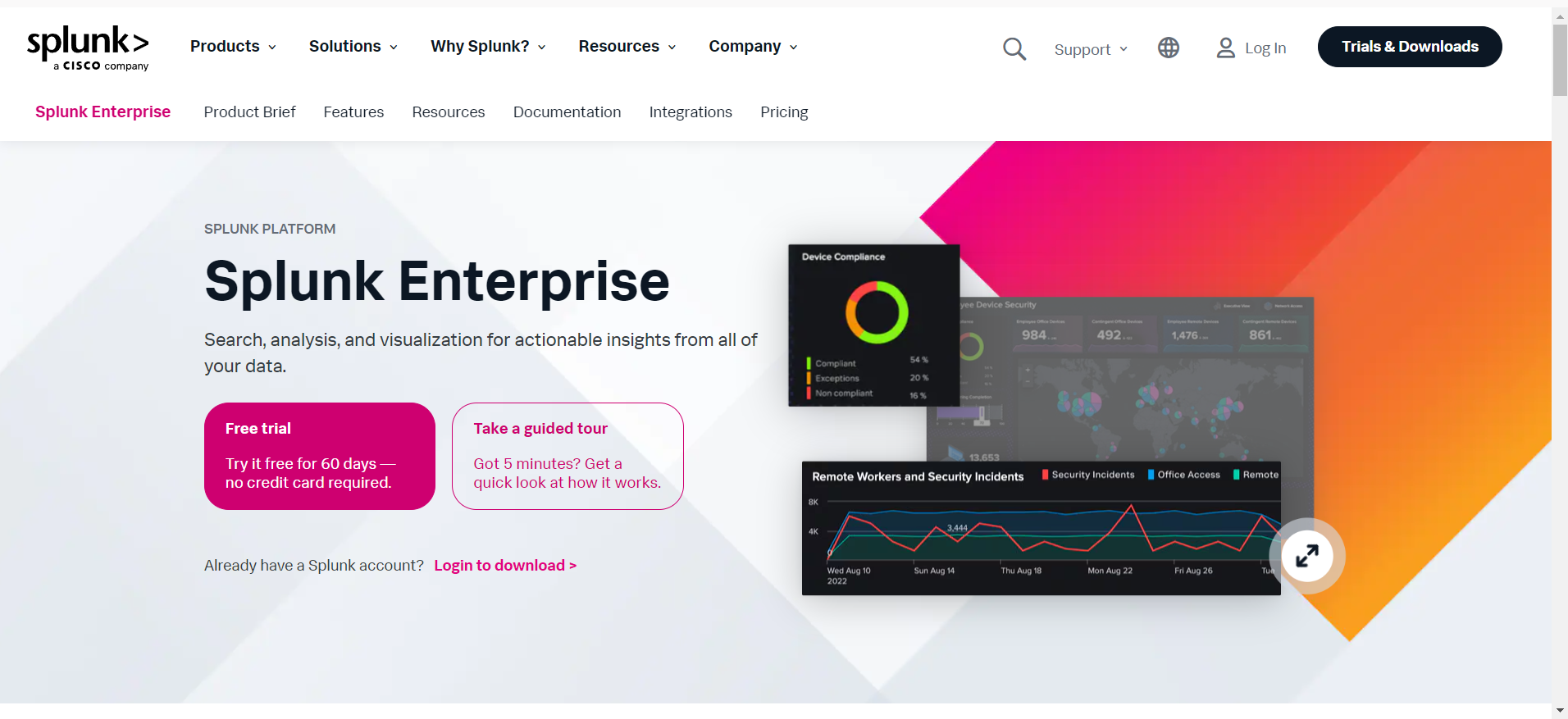
This step commands forwarder to forward which specific logs to splunk server.  
Add the following to /opt/splunkforwarder/etc/system/local/inputs.conf:  


[monitor:///var/log/syslog]  
disabled = false  
index = linux\_logs  
sourcetype = syslog  
  
[monitor:///var/log/auth.log]  
disabled = false  
index = linux\_logs  
sourcetype = linux\_secure

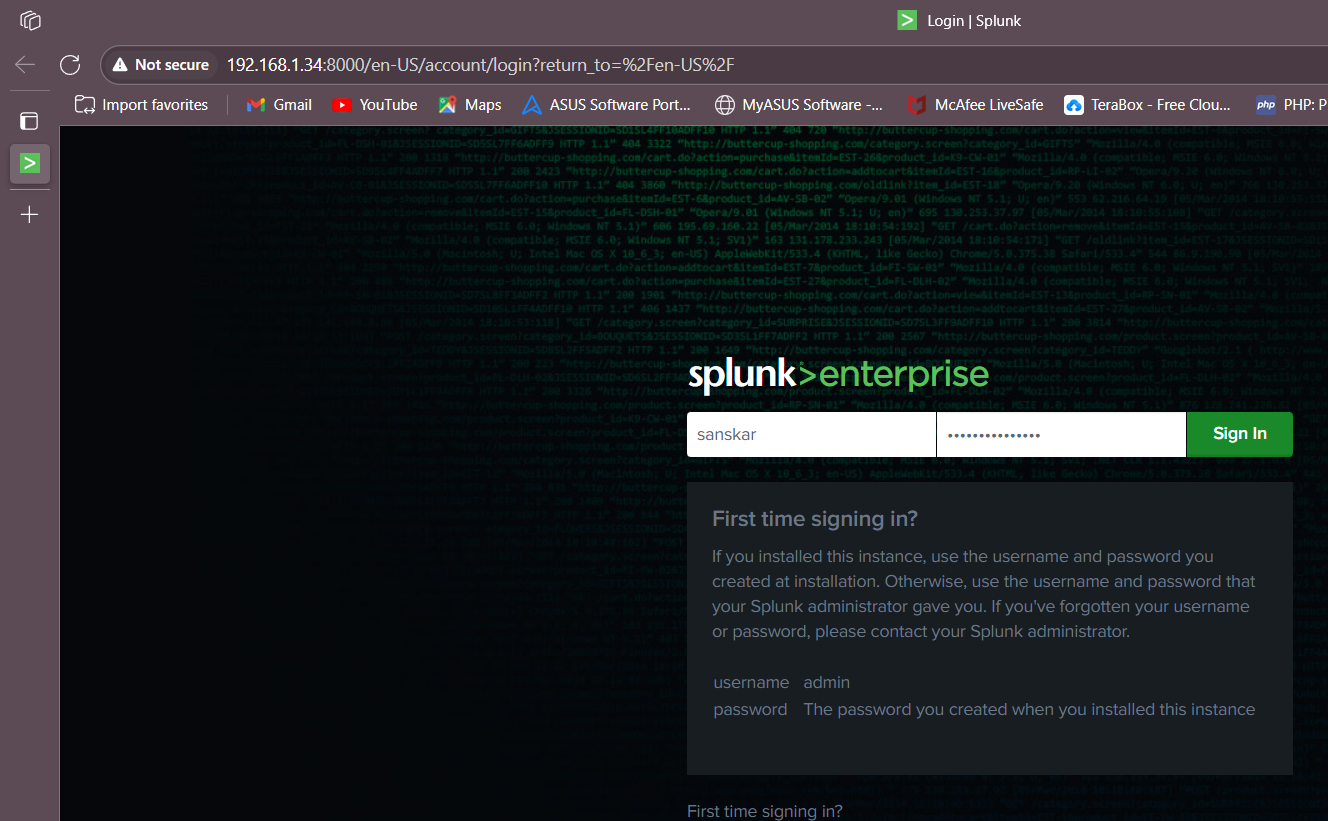
[monitor:///var/log/sysmon.log]  
disabled = false  
index = linux\_logs  
sourcetype = sysmon\_linux

# Splunk Enterprise Configuration

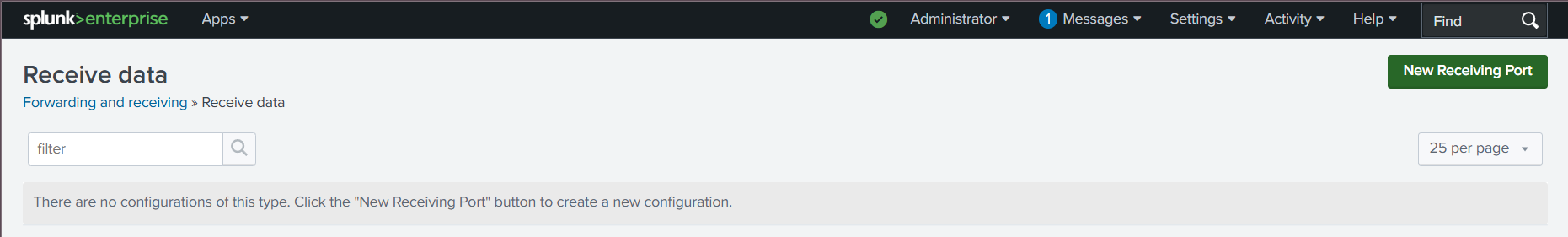
1. Download Splunk Enterprise for windows from official site :

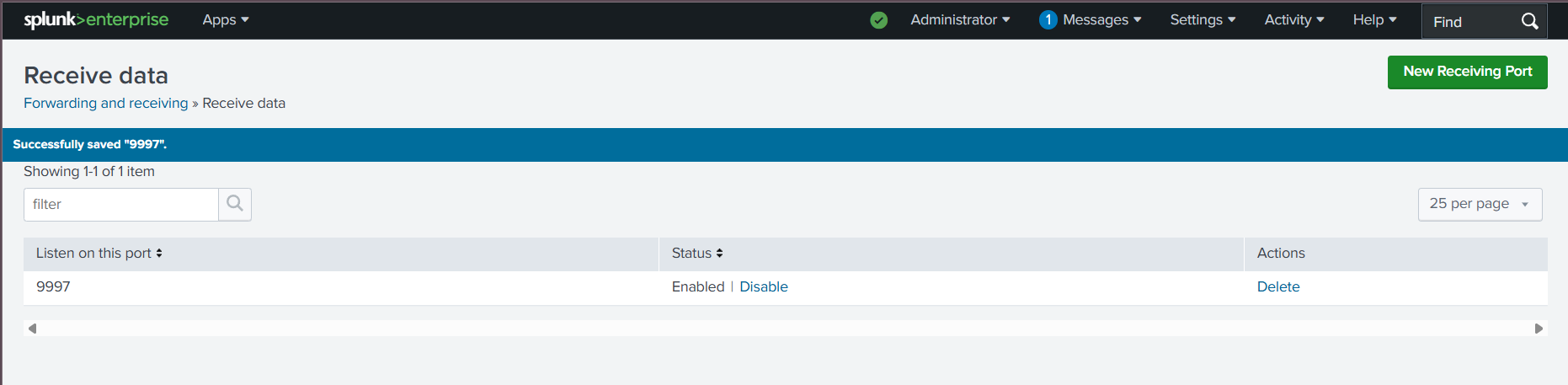


1. Set username and password to login on splunk server later.



1. Enable Receiving on Port 9997:

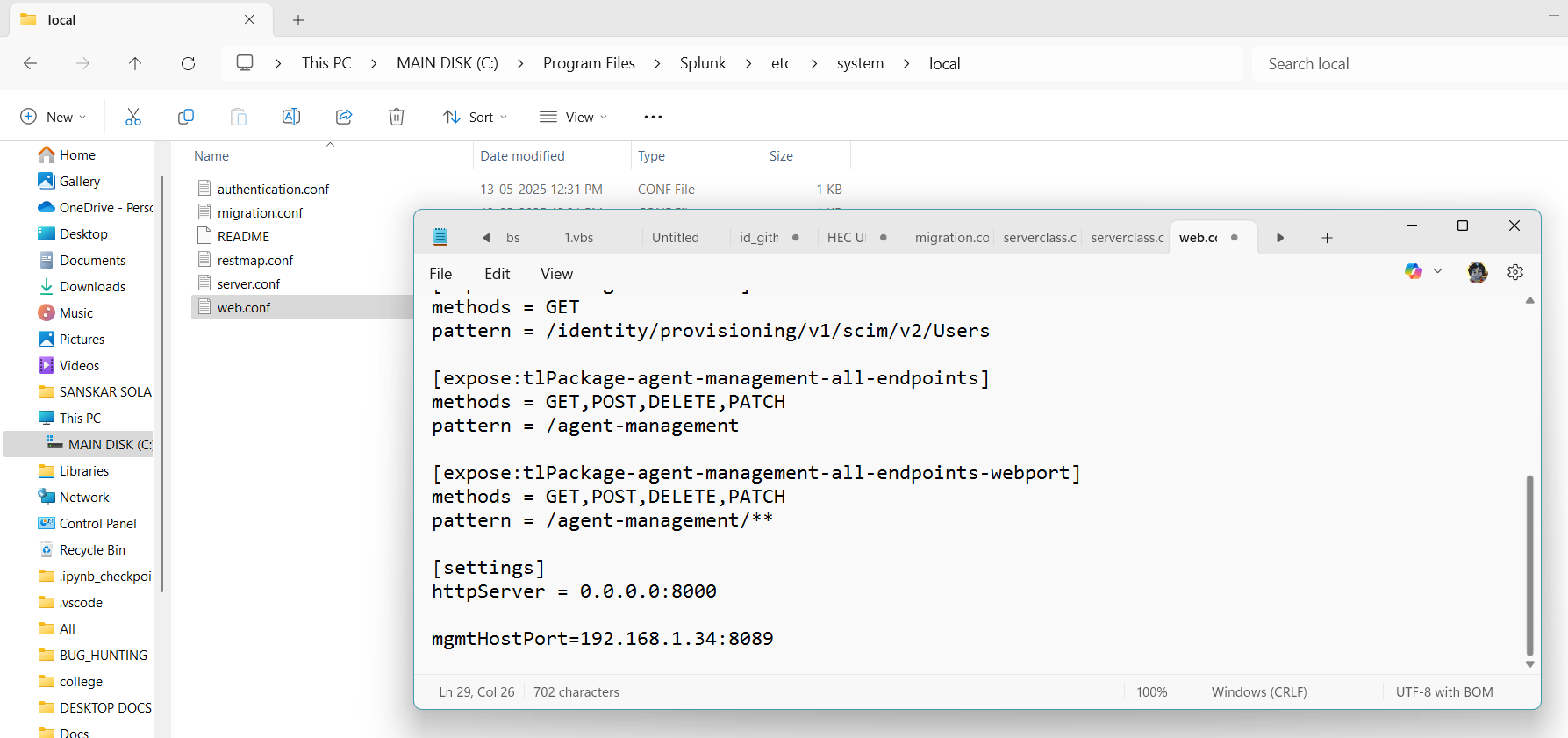




Settings > Forwarding and Receiving > Configure Receiving > new receiving port > Port 9997

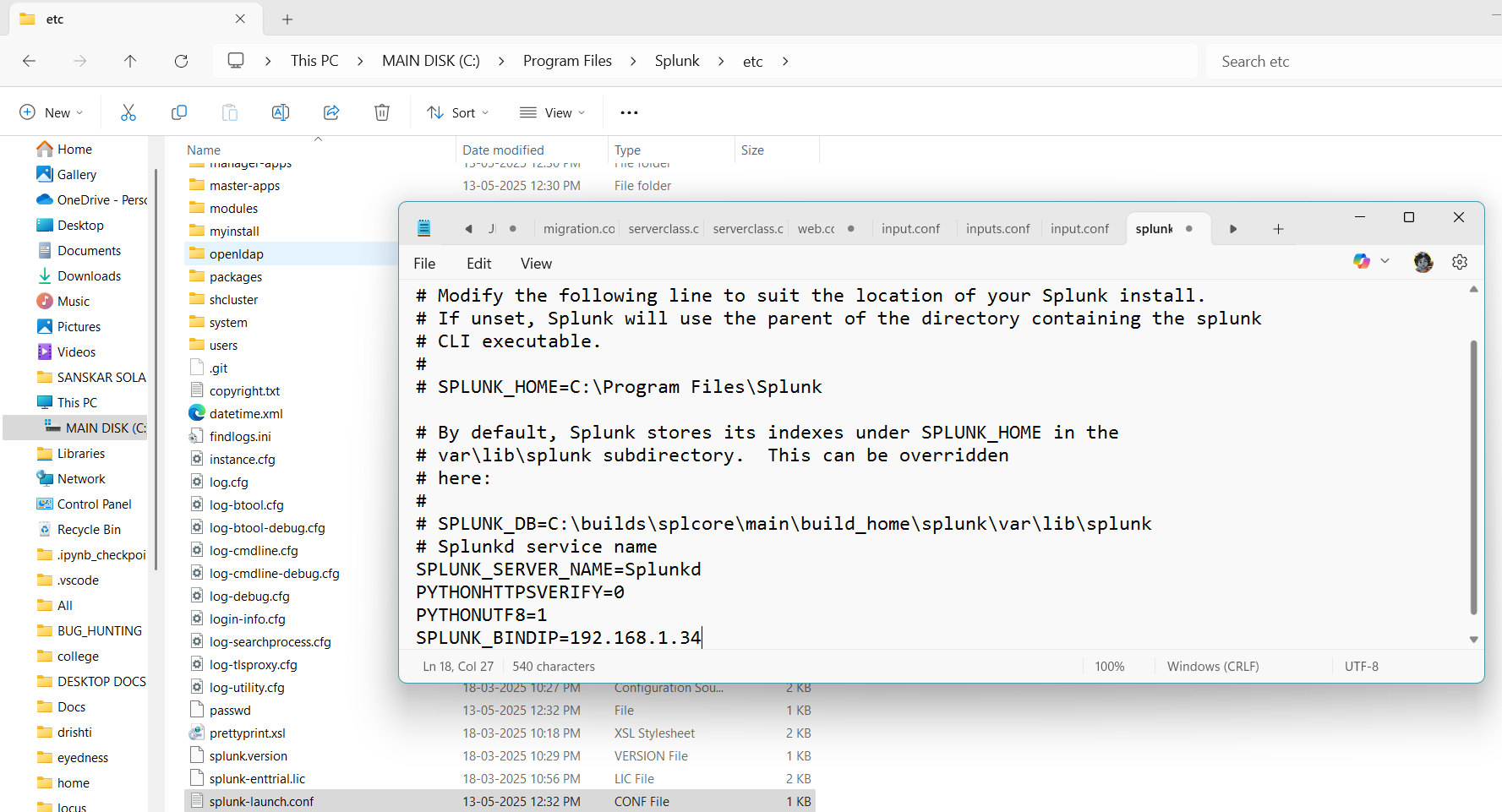
2. Configure web.conf :

To allow access to splunk forwarder in linux via actual IP of windows where splunk server is hosted , edit C:\Program Files\Splunk\etc\system\local\web.conf:

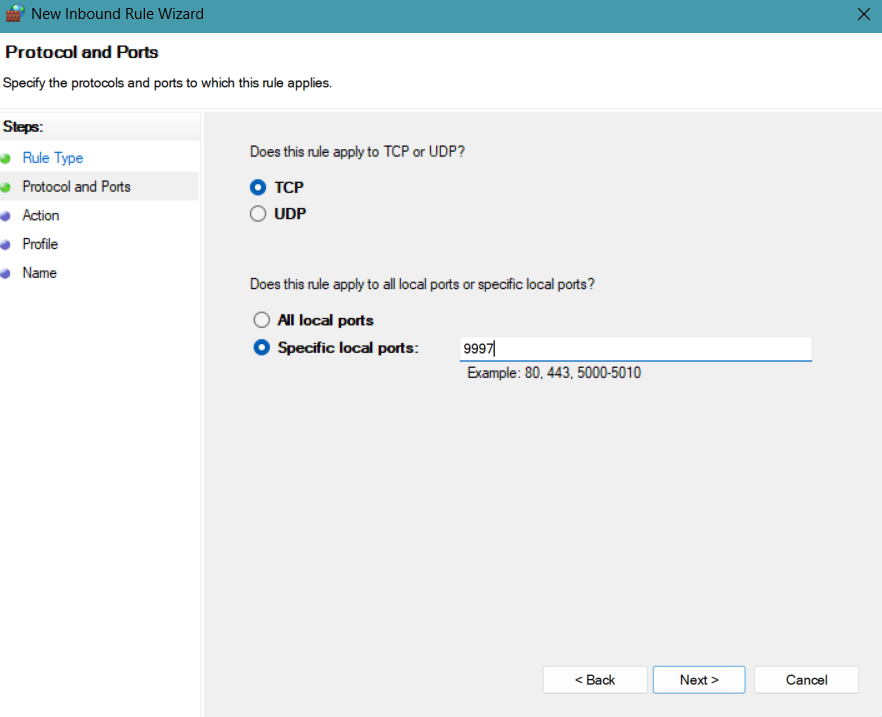


[settings]  
enableSplunkWebSSL = false  
httpport = 8000  
mgmtHostPort = 192.168.1.34:8089

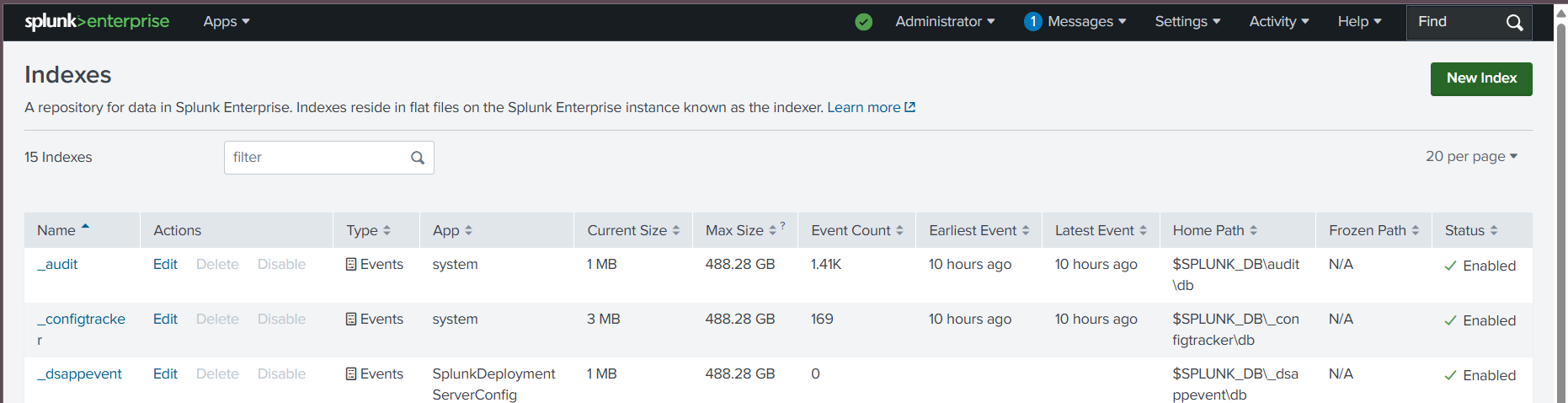
3. splunk-launch.conf :

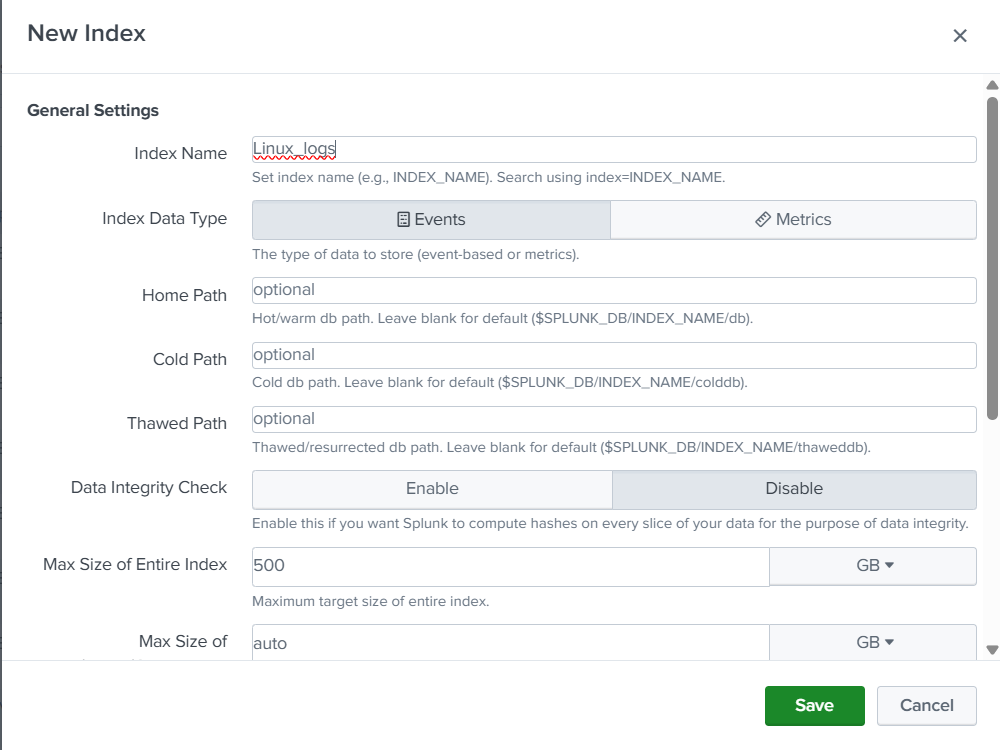
This is necessary , if we are changing IP in above step , to start splunk server with that actual IP.  
Configure environmental variables if needed in splunk-launch.conf , i.e , add bind\_ip.

1. Firewall Configuration(this is optional ):

Allow inbound connections on port 9997 (TCP) in Windows Defender Firewall.  


1. Create new index (namespace or data repository where forwarded logs are collected and analyzed ) in splunk enterprise , with name as linux\_logs.





1. Now restart splunk enterprise and splunk forwarder.

