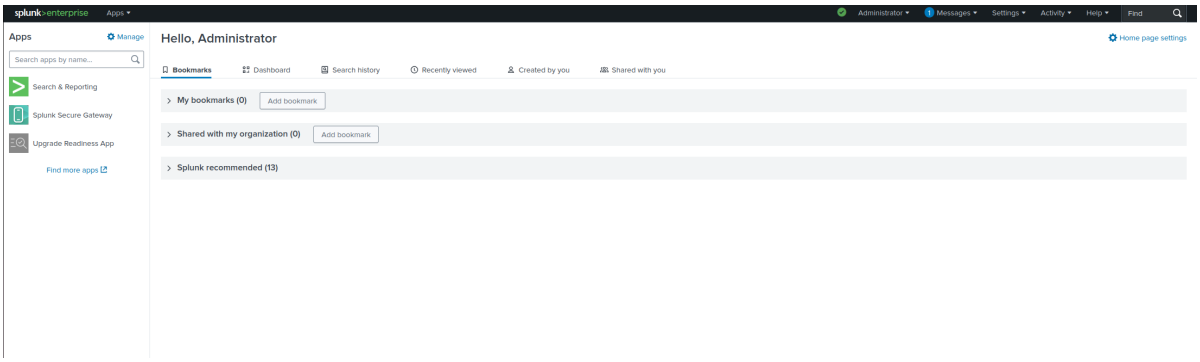
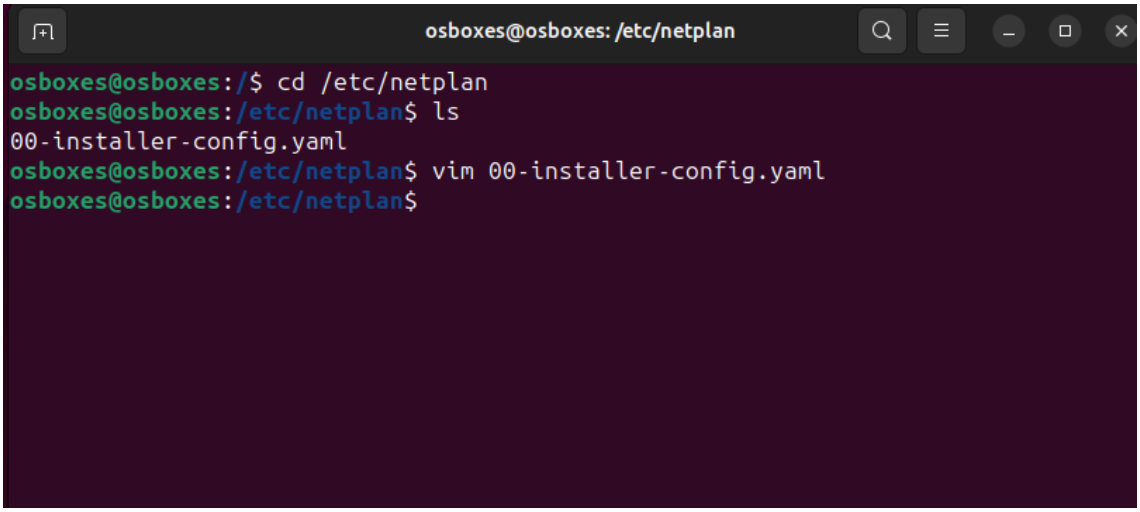
# Download and Install Splunk Enterprise on Ubuntu Server



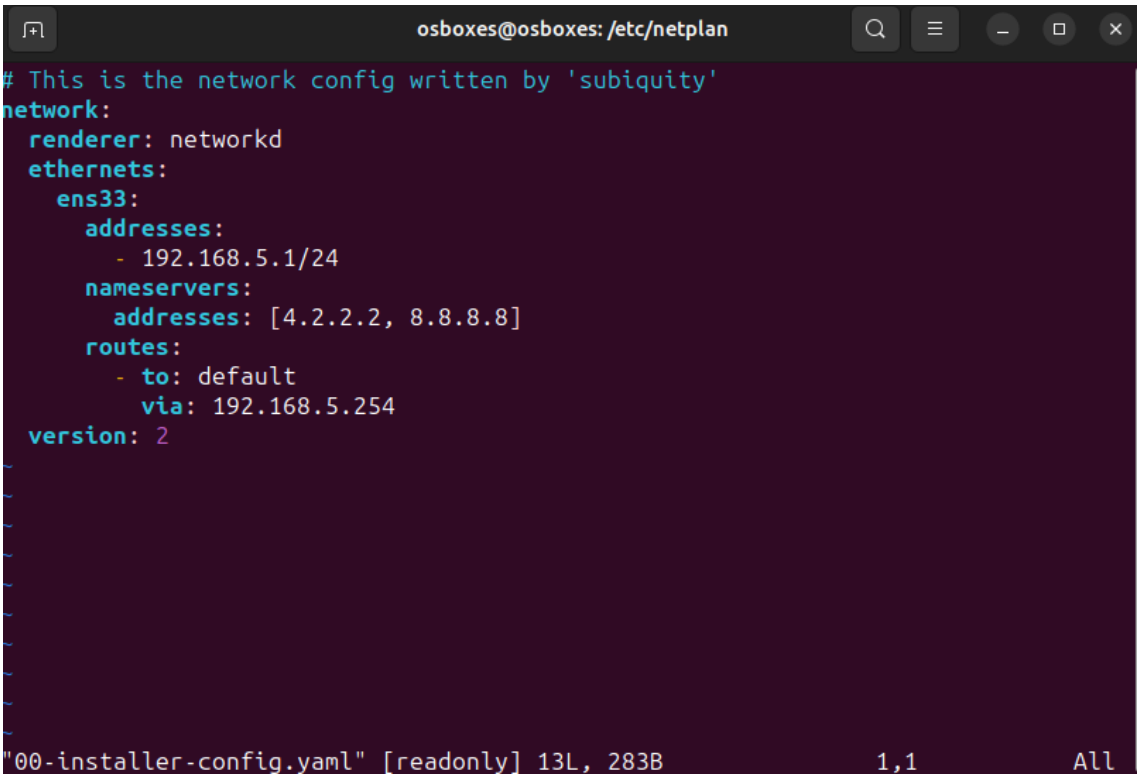

# Splunk Configuration

1. Setting Static IP address on Ubuntu Server, the objective is to keep ip address persistent upon each reboot



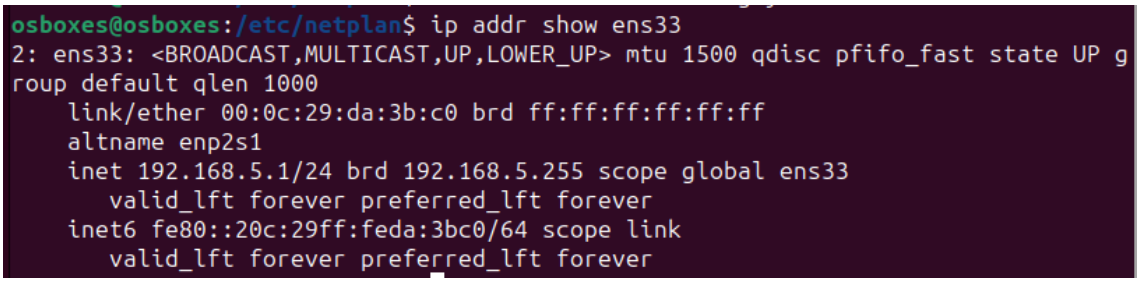

```
network:
 renderer: networkd
 ethernets:
 ens33:
 addresses:
 - 192.168.5.1/24
 nameservers:
 addresses: [4.2.2.2, 8.8.8.8]
 routes:
 - to: default
 via: 192.168.5.254
 version: 2
```

modify this file, change ip address to static instead of from dhcp server.

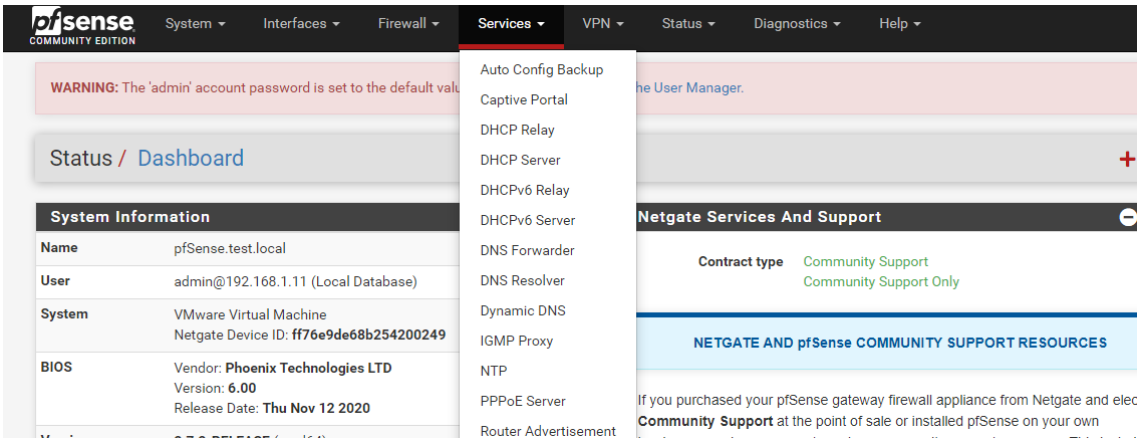



to make changes, execute command

```
netplan apply
ip addr show ens33
ip route show
```




2. Go to PfSense machine->login pfsense via link [http://192.168.1.254-](http://192.168.1.254-)>Services->DHCP Server




click SPLUNK, change address pool start IP to any IP other than 192.168.5.1, save and apply changes

ISC DHCP has reached end-of-life and will be removed in a future version of pfSense. Visit System > Advanced > Networking to switch DHCP backend.

LAN KALI SECONION SPLUNK

## General DHCP Options

| | |
|---|---|
| **DHCP Backend** | ISC DHCP |
| **Enable** | ☑ Enable DHCP server on SPLUNK interface |
| **BOOTP** | ☐ Ignore BOOTP queries |
| **Deny Unknown Clients** | Allow all clients<br>When set to **Allow all clients**, any DHCP client will get an IP address within this scope/range on this interface. If set to **Allow known clients from any interface**, any DHCP client with a MAC address listed in a static mapping on ***any*** scope(s)/interface(s) will get an IP address. If set to **Allow known clients from only this interface**, only MAC addresses listed in static mappings on this interface will get an IP address within this scope/range. |
| **Ignore Denied Clients** | ☐ Ignore denied clients rather than reject<br>This option is not compatible with failover and cannot be enabled when a Failover Peer IP address is configured. |
| **Ignore Client Identifiers** | ☐ Do not record a unique identifier (UID) in client lease data if present in the client DHCP request<br>This option may be useful when a client can dual boot using different client identifiers but the same hardware (MAC) address. Note that the resulting server behavior violates the official DHCP specification. |

## Primary Address Pool

| | |
|---|---|
| **Subnet** | 192.168.5.0/24 |
| **Subnet Range** | 192.168.5.1 - 192.168.5.254 |
| **Address Pool Range** | 192.168.5.10 (From) — 192.168.5.253 (To)<br>The specified range for this pool must not be within the range configured on any other address pool for this interface. |