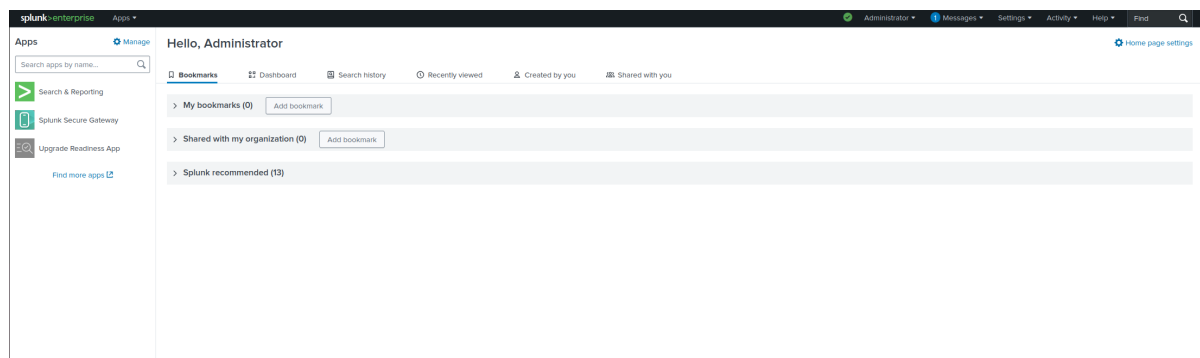


Download and Install Splunk Enterprise on Ubuntu Server



Splunk Configuration

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

```
osboxes@osboxes: /etc/netplan
osboxes@osboxes:/$ cd /etc/netplan
osboxes@osboxes:/etc/netplan$ ls
00-installer-config.yaml
osboxes@osboxes:/etc/netplan$ vim 00-installer-config.yaml
osboxes@osboxes:/etc/netplan$
```

```
network:
  renderer: networkd
  ethernet:
    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.

```
osboxes@osboxes: /etc/netplan
# This is the network config written by 'subiquity'
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

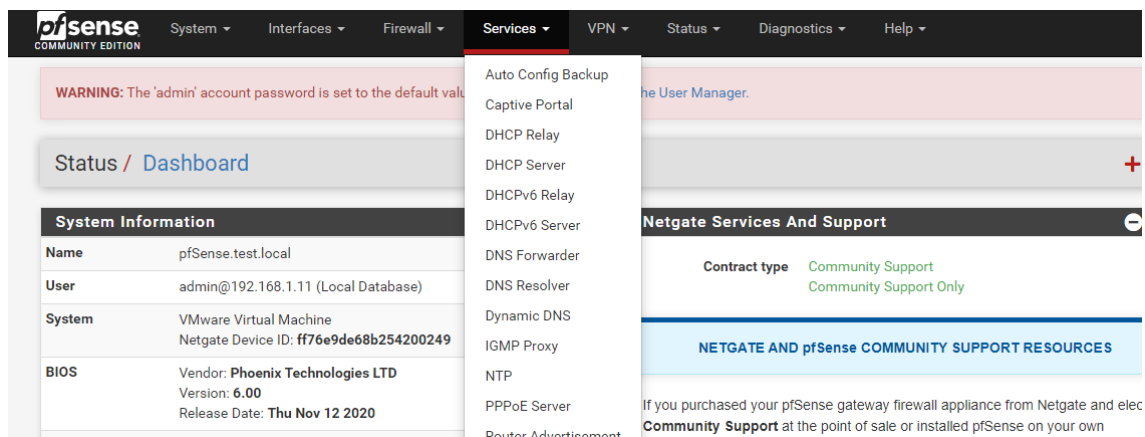
"00-installer-config.yaml" [readonly] 13L, 283B 1,1 All
```

to make changes, execute command

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

```
osboxes@osboxes: /etc/netplan$ ip addr show ens33
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP g
roup default qlen 1000
    link/ether 00:0c:29:da:3b:c0 brd ff:ff:ff:ff:ff:ff
    altname enp2s1
    inet 192.168.5.1/24 brd 192.168.5.255 scope global ens33
        valid_lft forever preferred_lft forever
    inet6 fe80::20c:29ff:feda:3bc0/64 scope link
        valid_lft forever preferred_lft forever
```

2. Go to PfSense machine->login pfsense via link <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	<input checked="" type="checkbox"/> Enable DHCP server on SPLUNK interface
BOOTP	<input type="checkbox"/> Ignore BOOTP queries
Deny Unknown Clients	<div>Allow all clients </div> <p>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.</p>
Ignore Denied Clients	<input type="checkbox"/> Ignore denied clients rather than reject This option is not compatible with failover and cannot be enabled when a Failover Peer IP address is configured.
Ignore Client Identifiers	<input type="checkbox"/> Do not record a unique identifier (UID) in client lease data if present in the client DHCP request 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	<div>192.168.5.10 </div> <div>From</div>	<div>192.168.5.253</div> <div>To</div>

The specified range for this pool must not be within the range configured on any other address pool for this interface.