Step-by-Step Indexer VM Installation Guide

This documentation will walk you through installing and setting up **Splunk Enterprise** on the **Index** VM.

Step 1: Downloading Splunk Enterprise
We need to first download the debian file splunk enterprise from their official website:
https://www.splunk.com/en_us/download/splunk-enterprise.html

NOTE: after downloading the .deb file. Do not ssh into the VM but have it's IP address for transfer

>> $————————————————————————[10 April 2025]

Step 2: copy the .deb from host to index VM
We need to copy the downloaded file from the host (do not ssh, use the host) to the VM and we gonna do that using or via ssh. To copy a .deb file (or any file) to your VM using scp, you need the following:

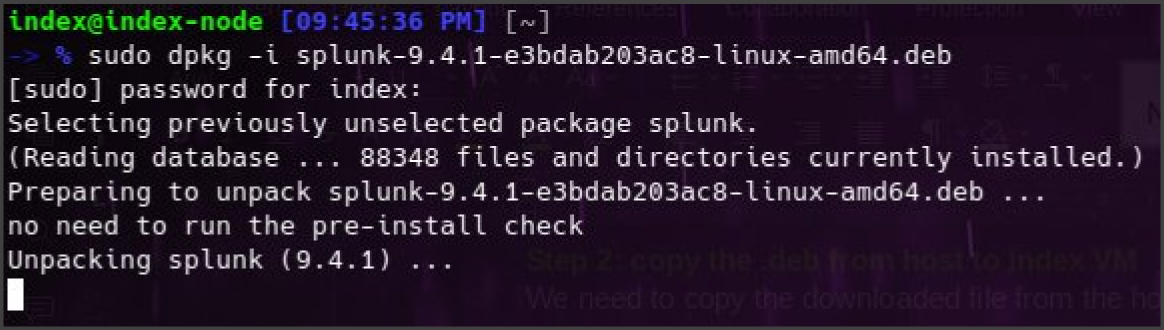
- IP address of the VM
- Username on the VM
- Path to the .deb file on your host machine

Then run the following command to copy the file:

```
scp ~/Downloads/splunk-enterprise.deb index@192.168.122.10:~
```

- Once the copy is done ssh into the VM, navigate to where you copied the file and run the following command to install splunk enterprise debian file:

  ```
  sudo dpkg – i splunk-enterprise.deb
  ```



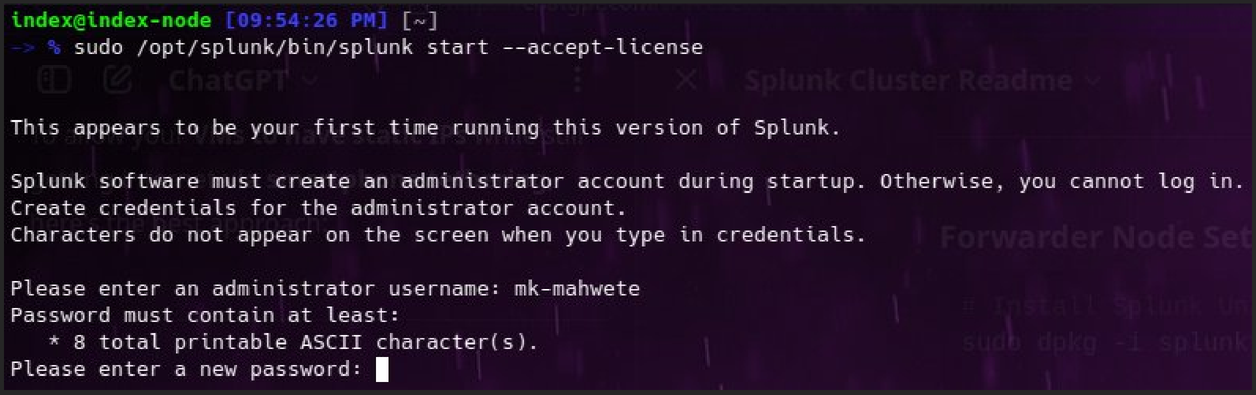
```
index@index-node [09:45:36 PM] [~]
-> % sudo dpkg -i splunk-9.4.1-e3bdab203ac8-linux-amd64.deb
[sudo] password for index:
Selecting previously unselected package splunk.
(Reading database ... 88348 files and directories currently installed.)
Preparing to unpack splunk-9.4.1-e3bdab203ac8-linux-amd64.deb ...
no need to run the pre-install check
Unpacking splunk (9.4.1) ...
```

>> $————————————————————————[10 April 2025]

Step 3: Configure the system to receive log files from the forward system

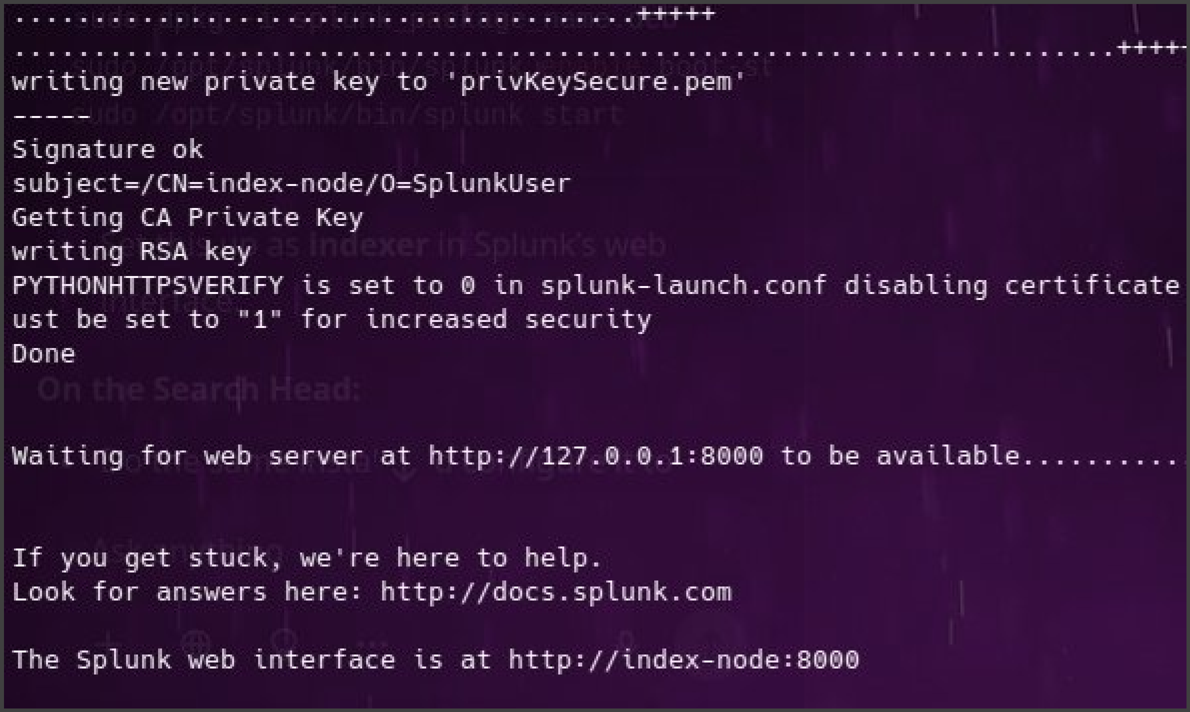
Before we even go feather we need to accept splunk terms and conditions (Licensing) and great an administrative username and password. Use the following command to accept the licensing agreement:

```
sudo /opt/splunk/bin/splunk start  – – accept-license
```



```
index@index-node [09:54:26 PM] [~]
-> % sudo /opt/splunk/bin/splunk start --accept-license

This appears to be your first time running this version of Splunk.

Splunk software must create an administrator account during startup. Otherwise, you cannot log in.
Create credentials for the administrator account.
Characters do not appear on the screen when you type in credentials.

Please enter an administrator username: mk-mahwete
Password must contain at least:
   * 8 total printable ASCII character(s).
Please enter a new password: 
```

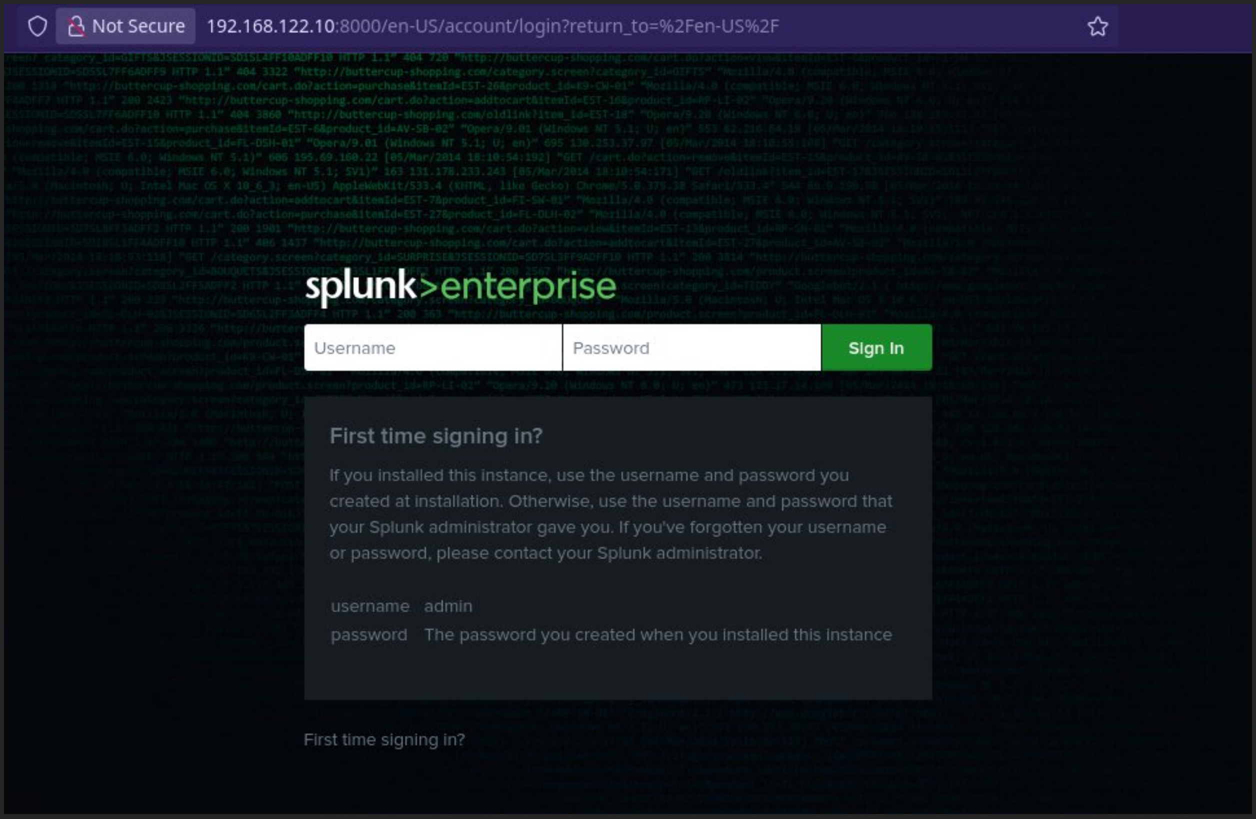
- Set a password you will remember because you gonna need it later on or when you want to login



```
.......................................+++++
......................................................................+++++
writing new private key to 'privKeySecure.pem'
-----
Signature ok
subject=/CN=index-node/O=SplunkUser
Getting CA Private Key
writing RSA key
PYTHONHTTPSVERIFY is set to 0 in splunk-launch.conf disabling certificate
ust be set to "1" for increased security
Done


Waiting for web server at http://127.0.0.1:8000 to be available..........


If you get stuck, we're here to help.
Look for answers here: http://docs.splunk.com

The Splunk web interface is at http://index-node:8000
```

- The installation and configurations is complete and now we have a web interface at **http://index-node** <or your VM IP address>**: 8000**

Now get the IP address of the index VM to test if the splunk we interface works: my VM IP is **192.168.122.10:8000** (make sure that port 8000 is open)



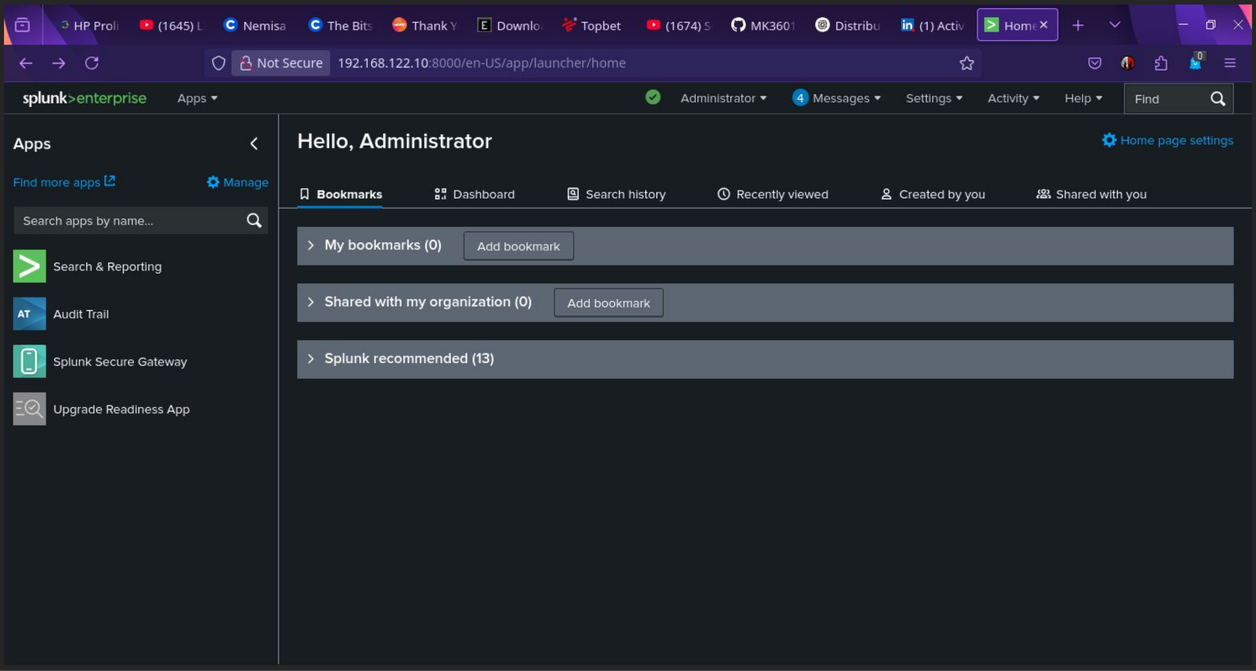
Not Secure 192.168.122.10:8000/en-US/account/login?return_to=%2Fen-US%2F

First time signing in?

If you installed this instance, use the username and password you created at installation. Otherwise, use the username and password that your Splunk administrator gave you. If you've forgotten your username or password, please contact your Splunk administrator.

username admin
password The password you created when you installed this instance

First time signing in?



Not Secure 192.168.122.10:8000/en-US/app/launcher/home

Hello, Administrator

My bookmarks (0)

Shared with my organization (0)

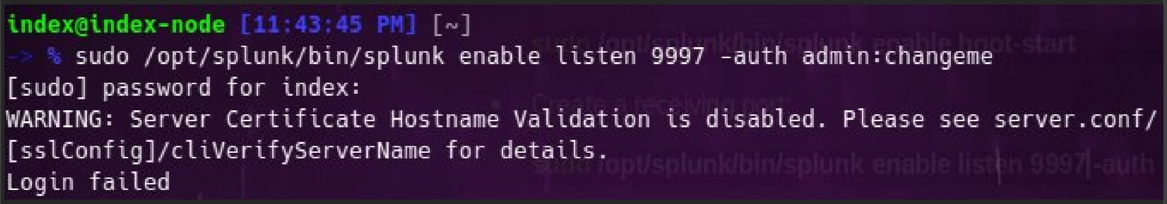
Splunk recommended (13)

- Enable boot start:

```
sudo /opt/splunk/bin/splunk enable boot-start
```

- Create a receiving port:

```
sudo /opt/splunk/bin/splunk enable listen 9997 -auth admin:changeme
```



```
index@index-node [11:43:45 PM] [~]
-> % sudo /opt/splunk/bin/splunk enable listen 9997 -auth admin:changeme
[sudo] password for index:
WARNING: Server Certificate Hostname Validation is disabled. Please see server.conf/
[sslConfig]/cliVerifyServerName for details.
Login failed
```

This error occurs because I have to use my admin name and password: **sudo /opt/splunk/bin/splunk enable listen 9997 -auth 'mk-mahwete:@LmiCh*alMk'**

After this command, port **9997** should now work fine because the Indexer is now listening for data from forwarders on port 9997.